جامعة الإسراء

كلية الحقوق

الدراسات العليا

جريمة التزوير الالكتروني

"دراسة تحليلية مقارنة"

electronic forgery crime

"A comparative analysis study"

اعداد

نافل عبد الكريم العقلة الفالح

اشراف

الدكتور اكرم الفايز

استاذ القانون الجنائي المشارك

قدمت هذه الرسالة لاستكمال متطلبات الحصول على درجة الماجستير في القانون

كلية الحقوق

جامعة الاسراء

كانون اول 2014

قرار لجنة المناقشة

نوقشت رسالة الماجستير للطالب نافل عبد الكريم العقلة الفالح بتاريخ / / 2014 والموسومة بـــــي جريمة التزوير الالكتروني "دراسة تحليلية مقارنه" .

وأجيزت بتاريخ / / 2014 .

اعضاء لجنة المناقشة :-

اسم العضو	التوقيع

تفويض

انا الطالب نافل عبد الكريم العقلة الفالح ، أفوض جامعة الاسراء بتزويد نسخ من رسالتي للمكتبات او المؤسسات او الهيئات او الاشخاص عند طلبها .

التوقيع :

التاريخ :

قال العماد الاصفهاني :-

" اني رأيت انه لا يكتب احد كتابا في يومه الا قال في غدو، لو غير هذا لكان احسن ، ولو زيد هذا لكان يستحسن ، ولو قدم هذا لكان افضل ، ولو ترك هذا لكان اجمل ، وهذا من اعظم العبر وهو دليل على استيلاء النقص على جملة البشر "

الاهداء

الى روح والدي الطاهرة ،،

الى روح والدتي الطاهرة ،،

الى عائلتي (زوجتي وابنائي) ،،

شكر وتقدير ،،،

اتقدم بجزيل شكري وامتناني الى السادة رئيس واعضاء لجنة المناقشة الكريمة على تجشمهم عناء قراءة وتدقيق وضبط وتقييم هذا الجهد المتواضع وعلى دورهم الرئيس في تجويد المحتوى وسلامة النتائج.

كما اتقدم بشكري وامتناني للمشرف الفاضل الدكتور اكرم الفايز استاذ القانون الجنائي المشارك على ما قدمه من دعم واسناد بغية انجاز هذه الرسالة بالصورة التي خرجت فيها .

وكل الشكر والتقدير للاسرة والاهل وجميع من ساندي في دراستي.

آملا للجميع كل التوفيق والنجاح .

والله ولي التوفيق

فهرس المحتويات

الموضوع	الصفحة
قرار لجنة المناقشة	ب
نموذج التفويض	ج
قول مأثور	د
الاهداء	ه
الشكر والتقدير	و
فهرس المحتويات	ز
الملخص باللغة العربية	ط
المقدمة	1
الفصل التمهيدي :- نشأة التزوير الالكتروني والاتجاهات التشريعية لتنظيمة	7
المبحث الاول :- نشأة وتطور التزوير الألكتروني	9
المطلب الاول :- نشأة التزوير الالكتروني	10
المطلب الثاني :- تطور التزوير الالكتروني كاحد صور الجرائم الالكترونية	13
المبحث الثاني :- الاتجاهات التشريعية الدولية والوطنية لتنظيم التزوير الالكتروني	16
المطلب الاول :- الاتجاهات الدولية لتنظيم التزوير الالكتروني .	19
المطلب الثاني :- الاتجاهات الوطنية لتنظيم التزوير الالكتروني .	23
الفصل الاول :- ماهية التزوير الالكتروني	26
المبحث الاول :- تعريف ومحل التزوير الألكتروني	27
المطلب الاول :- تعريف التزوير الالكتروني	28
المطلب الثاني :- محل التزوير الالكتروني	32
المبحث الثاني :- صور جريمة التزوير الألكتروني .	37
المطلب الاول :- صور التزوير الالكتروني بالنظر الى محل الجريمة .	39
المطلب الثاني :- صور التزوير الالكتروني بالنظر الى طريقة ارتكاب الفعل.	45
الفصل الثاني :- اركان جريمة التزوير الالكتروني وموقف القانون الاردني منها.	48

المبحث الاول :- الركن المادي و الركن المعنوي لجريمة التزوير الالكتروني	50
المطلب الاول :- عناصر الركن المادي لجريمة التزوير الالكتروني	51
المطلب الثاني :- عناصر الركن المعنوي لجريمة التزوير الالكتروني	57
المبحث الثاني :- موقف القانون الاردني من جريمة التزوير الالكتروني بوصفها من جرائم انظمة المعلومات .	59
المطلب الاول :- جريمة التزوير الالكتروني في ظل قانون المعاملات الالكترونية	60
المطلب الثاني :- جريمة التزوير الالكتروني في ظل قانون جرائم انظمة المعلومات	70
الخاتمة	77
التوصيات	79
المراجع	81
ملخص الرسالة باللغة الانجليزية	87
ملحق قانون جرائم انظمة المعلومات الاردني	88

جريمة التزوير الالكتروني

"دراسة تحليلية مقارنة "

اعداد الطالب نافل عبد الكريم العقلة الفالح

المشرف

الدكتور اكرم الفايز

استاذ القاون الجنائي المشارك

ملخص

لقد كان لتطور تطبيقات تكنولوجيا المعلومات بدءا من اختراع الكمبيوتر ومرورا بالحاسوب الشخصي وليس انتهاء بالشبكات والانترنت ، اثر في تطور وسائل ارتكاب الجرائم بوجه عام ومن ضمنها جريمة التزوير الالكتروني . وقد نشأ في نطاق الجرائم الالكترونية جريمة التزوير الالكتروني التي تعتمد على الكمبيوتر كاداة لارتكابها وايضا ترتكب على الملفات والبيانات المخزنة داخل انظمة الكمبيوتر ، وهذا ما يعرف بالتزوير الالكتروني .

وفي سياق هذا الوصف ، فان جرائم التزوير الالكتروني ، تستهدف تغيير الحقيقة في الملفات او السجلات او المستندات المعالجة الكترونيا المحفوظة لدى الغير او الخاصة بالغير او تستهدف اصطناع ملفات لا وجود لها وتغاير الحقيقة ،وهي تنسب الى طائفة الجرائم التي يلعب الكمبيوتر فيها دور الوسيلة او الاداة التي تتيح وتسهل ارتكاب الفعل ، وان كانت مقارفتها ابتداء تقوم باستخدام وسائل وتطبيقات تكنولوجيا المعلومات وتوجه ايضا الى معطيات مخزنة او معالجة او منقولة عبر نظم المعلومات .

ونقف هنا على جريمة التزوير الالكتروني بوجه عام ، ماهيتها وصورها واركانها وعناصرها وما يدخل في نطاقها بالنظر الى محلها ومراحل تطورها ، بالأضافة الى بيان اهم المعالجات التشريعية الدولية و الوطنية التي تصدت لهذه الجريمة المبتكرة .

جريمة التزوير الالكتروني

المقدمة

إنّ من أهم إنجازات العلم الحديث في هذا العصر وأعظمها جدوى للإنسان ظهور الحاسب الآلي والإنترنت ، وماحقّقته تكنولوجيا المعلومات و الاتصالات من فوائد عديدة في مجال الرقيّ والتقدُّم الإنساني في أغلب مناحي الحياة الاقتصادية والتعليمية والطبية وكافة المجالات الأخرى.

لكن رافق هذه الانجازات بروز اشخاص يتمتعون بالخبرة والحرفية في تطويع هذه التقنية للقيام بأعمال إجرامية أفرزت إلى جانب الجريمة التقليدية الجرائم المعاصرة ، بلحوّلت هذه الجريمة من صفتها العاديّة وأبعادها المحدودة إلى أبعاد جديدة تعتمد التقنية في تنفيذ الفعلالمجرّم ، وبأساليب مبتكرة، وطرق جديدة لم تكن معروفة من قبل.

وساعد هؤلاء المجرمون ما يشهده العصر من تطور الوسائل المعلوماتية الحديثة ، في زيادة سرعة نشر جرائمهم حتى أصبحت تهدد تكنولوجيا المعلومات ذاتها ،حيث أصبح في إمكانهم التسبُّب في خلق شلل كامل للأنظمة الالكترونية المدنيّة والعسكريّة، الأرضيّة والفضائيّة، وتعطيل المعدّات الإلكترونيّة المختلفة ، واختراق النُّظم المصرفيّة، وإرباك حركة الطيران وشل محطات الطاقة وغيرها بواسطة قنابل معلوماتية ترسلها لوحة مفاتيح الكمبيوتر من على مسافات تتعدّى عشرات الآلاف من الأميال، وذلك دون أن يترك المجرم المعلوماتي أو الإلكتروني أثرًا ملموسًا لملاحقته ومعرفةمَصدرها. والجاني يستطيع بواسطة هذه التقنيات العالية أن يصل إلى أي مكان يرغب فيه ، عبر الإبحار في الشبكة المعلوماتية ويتصل ويتفاعل مع من شاء في أي مكان ، فلا مكان ولا زمان يستطيع وضع حدود لهذه الشبكة.

و ان الكمبيوتر يلعب ثلاث ادوار رئيسة في نطاق الجرائم الالكترونية ، فهو قد يكون **هدفها ومحلها** ، وهذا يتحقق في الصور الجرمية التي تستهدف سرية وسلامة وتوفر معطيات الكمبيوتر المخزنة او المعالجة داخل نظام الكمبيوتر، كجرائم الدخول غير المصرح به الى نظم المعلومات وجرائم اتلاف المعطيات (خاصة بتقنية الفايروسات او البرامج الخبيثة) ، وجرائم تعطيل النظم وانكار الخدمات واعتراض البيانات وغيرها. وقد يكون نظام المعلومات او الكمبيوتر **الوسيلة**

او الاداة لارتكاب الجريمة، كجرائم التزوير الالكتروني والاحتيال الالكتروني، حيث يسخر فيها الكمبيوتر كوسيلة لارتكاب الجريمة ، **وقد يكون مجرد بيئة للجريمة**، كسائر جرائم المحتوى الضار لمواقع المعلوماتية التي يتيح الكمبيوتر كجزء من الشبكات بيئة لمقارفة الفعل وتحقق نتائجه ، كما في مواقع ترويج المواد الاباحية او موقع انشطة القمار او غسل الاموال او الاتجار بالاسلحة او الاتجار بالبشر وغيرها من المواقع ذات المحتوى الضار في بيئة الانترنت.

ولخطورة جريمة التزوير الالكتروني ، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (**بيانات ، ومعلومات ، وبرامج بكافّة أنواعها**) ، فهي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء ، يمتلكون أدوات المعرفة التقنية،ذو وَجَّه للنَّيْل مِنَ الحق في المعلومات، وتَطَال اعتداءاتها معطيات الكمبيوتر المخزّنة ، والمعلومات المنقولة ، عبر نُظُم وشبكات المعلومات ، وفي مقدمتها الإنترنت ، **تم** التصدي اليها منذ السبعينات التي بدأت تشهد تدخلات تشريعية لمواجهة اساءة استخدام الكمبيوتر وبنوك المعلومات ، اما الجهد الدولي فلم يتحقق فعليا الا في تسعينات القرن المنصرم ولا يزال دون المستوى المطلوب بالقياس بالجهود الاقليمية والوطنية .

و تعتبر السويد اول دولة تسن تشريعات ضد (جرائم الكمبيوتر) او ما اصبح يعرف لاحقا بالجرائم الالكترونية او جرائم المعلوماتية ، لاسيما التزوير الاكتروني ، حيث صدر قانون البيانات السويدي عام (1973) الذي عالج قضايا الدخول غير المشروع للبيانات الحاسوبية او تزويرها أو تحويلها او الحصول غير المشروع عليها .

وعلى مستوى الدول العربية ، فقد قامت بعض الدول بسن قوانين خاصة بجرائم الحاسوب والانترنت ، تعددت تسمياتها واختلفت ، والاكثر شيوعا من حيث التسمية (جرائم انظمة المعلومات) ، وقد شملت بفقراتها التزوير الالكتروني او المعلوماتي كما هو الحال في دولة الامارات العربية التي تعد من اوائل الدول العربية التي تسن قانون مكافحة الجرائم المعلوماتية رقم 2 لسنة 2006 ، وتأتي المملكة العربية السعودية لتسن نظام مكافحة الجرائم المعلوماتية وذلك في جلسة مجلس الوزراء المنعقدة في 7 ربيع الاول 1428 هـ .

اما في الاردن ، ولاغراض مواجهة الجرائم الالكترونية والتي تعد جريمة التزوير الالكتروني من ابرزها ، تم في عام 2010 سن قانون جرائم انظمة المعلومات الاردني المؤقت رقم 30 لسنة 2010 ، وكان من المتوقع ان يغطي هذا القانون القدر الملائم والمناسب من صور

الجرائم الالكترونية المختلفة ،الا ان القانون المؤقت جاء محدوداً من حيث الجرائم التي نص عليها من بين الجرائم الالكترونية ، وجاءت معالجته للتزوير الالكتروني تحديدا اقل من المتوقع .

اهمية الدراسة :-

تكمن اهمية الرسالة في التعرض لقانون انظمة المعلومات الاردني بوصفة القانون الخاص الذي ينظم جريمة التزوير الالكتروني وباقي الجرائم الالكترونية ، ويحدد الافعال التي يمكن ان تتناولها نصوص التجريم ، كما تكمن اهمية الرسالة في تسليط الضوء على اوجه القصور و النقص في هذا القانون من حيث اغفال النص على الكثير من الصور الجرمية لجريمة التزوير الالكتروني كما هو الحال في العديد من الدول ،وكذلك معرفة اوجهة الاختلاف بين جريمة التزوير التقلدية او العادية وبين جريمة التزوير الالكتروني من حيث الاركان و العناصر وما يدخل في نطاقها ، و من حيث محل الجريمة (محل الاعتداء) ، والقانون الواجب التطبيق على هذه الجرائم المبتكرة .

اهداف الدراسة :-

أن هذا الرسالة تهدف الى الوقوف على جريمة التزوير الالكتروني بوجه عام ، ماهيتها وصورها واركانها وما يدخل في نطاقها بالنظر الى محلها ، و تهدف كذلك الى بيان الاتجاهات الدولية والوطنية المقارنة للتصدي للتزوير الالكتروني من خلال تجريم شتى صوره ، واتناول اخيرا موقف القانون الاردني من جريمة التزوير الالكتروني في ضوء احكام قانون جرائم انظمة المعلومات المؤقت رقم 30 لسنة 2010 ، وقانون المعاملات الالكترونية المؤقت رقم 85 لسنة 2001 .

مشكلة الدراسة :-

ان مشكلة الدراسة تكمن في تسليط الضوء على قانون جرائم انظمة المعلومات الاردني بوصفة القانون الذي تناول ضمن نصوصة جريمة التزوير الالكتروني ، حيث نتناول الصور الجرمية التي نص عليها هذا القانون المتعلقة بجريمة التزوير الالكتروني ، وكذلك اوجة النقص و القصور في تناول صور هذه الجريمة .

اشكالية الدراسة :-

تكمن الاشكالية في هذه الدراسة بقلة المراجع المتخصصة التي تناولت جريمة التزوير الالكتروني بشكل مفصل ومستقل عن باقي جرائم انظمة المعلومات ، حيث ان جميع هذه المراجع قد تناولت

هذه الجريمة بالقليل من الايجاز وعند التطرق لها كان فقط لأغراض خدمة التسلسل العلمي لأبحاثهم او دراساتهم فقط .

محددات الدراسة :-

لا تتناول هذه الدراسة الجوانب الاجرائية لجريمة التزوير الالكتروني التي تتعلق بطرق التحقيق الابتدائي و الضبط و التفتيش و الخبرة الفنية التي تتطلبها هذه الجريمة ، حيث ان هذه الجريمة لها طبيعة خاصة و أدلتها غير محسوسة و تحتاج لخبرة فنية متخصصة عند اجراء الضبط و التفتيش ،حيث ان اجراءات الضبط التفتيش بمثل هذا النواع من الجرائم تختلف عن الاجراءات المطلوبة في الجرائم العادية او التقلدية وهي و تتطلب تقنية عالية من اجل تنفيذها بشكل صحيح ، لذلك يجب ان يكون الاشخاص الذين يباشرون اجراءات الضبط و التفتيش على قدر عالي من المعرفة التقنية لمحتويات الكمبيوتر ومكوناته ، وبعكس ذلك فأنه من غير الممكن اثبات الجريمة المعلوماتية .

الدراسات السابقة :-

اما عن الدراسات السابقة التي تناولت موضوع الرسالة فلم اجد الكثير من الدراسات او الابحاث السابقة التي تعاملت مع مشكلة البحث (جريمة التزوير الالكتروني) بشكل تفصيلي ودقيق ، على الرغم من وجود العديد من البحوث والكتب التي تتناولت جريمة التزوير ضمن شرح جرائم الكمبيوتر او جرائم المعلومات بشكل عام ولكنها لم تأتي على هذه الجريمة بشي من التفصيل و التحليل بل جاء التطرق اليها بشكل مختصر :-

1- محمد علي العريان ، الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، 2000 ، كما ان هذه الدراسة على الرغم من انها قد تناولت جرائم انظمة المعلومات الا انها لم تفصل جريمة التزوير الالكتروني من حيث الماهية و الاركان و العناصر و المحل .
2- محمد محي الدين عوض،مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)،ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي،القاهرة ،25-28 تشرين اول 1993 ، ونجد هنا ان هذه الدراسة قد تحدثت عن الاطار العام لجرائم نظم المعلومات (الكمبيوتر) ، ولم تتطرق الى جريمة التزوير الالكتروني بما يتح التعرف على هذه الجريمة و مدى اهتمام التشريعات الدولية و الوطنية بتنظيم احكام هذه الجريمة .

منهج الدراسة :-

ونتبع في هذه الرسالة المنهج الوصفي و التحليلي للنصوص القانونية ، كما يتبع الباحث المنهج المقارن لأغراض خدمة الرسالة المتصلة بمشكلتها الرئيسة .

منهجية الدراسة :-

لقد تم تناول هذه الدراسة من خلال ثلاث فصول ، تناول الفصل التمهيدي نشأة التزوير الالكتروني والاتجاهات التشريعية لتنظيمة ، و الفصل الاول تناول ماهية التزوير الالكتروني ، والفصل الثاني تناول اركان جريمة التزوير الالكتروني وموقف القانون الاردني من هذه الجريمة ، وجاء التقسيم على النحو التالي :-

فصل تمهيدي :- نشأة التزوير الالكتروني والاتجاهات التشريعية لتنظيمة ، وفيه اعرض لنشأة وتطور التزوير الالكتروني في المبحث الاول ، ومواقف الجهات الدولية و الوطنية من المعالجة التشريعية لهذه الجريمة في المبحث الثاني.

الفصل الاول :- ماهية التزوير الالكتروني ، وفيه اتناول تعريف ومحل التزوير الألكتروني في المبحث الاول . وصور التزوير الألكتروني في المبحث الثاني .

الفصل الثاني :- اركان جريمة التزوير الالكتروني وموقف القانون الاردني من جريمة التزوير الالكتروني ، وفيه اتناول الركن المادي والركن المعنوي لجريمة التزوير الالكتروني في المبحث الاول ، وموقف القانون الاردني من جريمة التزوير الالكتروني في ضوء قانون جرائم انظمة المعلومات ،وقانون المعاملات الالكترونية الاردني في المبحث الثاني .

آمل ان تحقق هذه الرسالة غرضها معتذرا عن اي قصور في ضوء الصعوبات المحيطة بالموضوع .

الباحث

فصل تمهيدي

نشأة التزوير الالكتروني والاتجاهات التشريعية لتنظيمة

تمهيد وتقسيم :-

ان الجرائم الالكترونية ، ظاهرة حديثة النشأة لأرتباطها بتكنولوجيا حديثة هي تكنولوجيا الحاسب الآلي التي لم تكن مألوفة من قبل وخاصة في بدايات القرن الماضي . ونتيجة لاستخدام الحاسب الآلي ومن ثم شبكات المعلومات التي ربطت بين هذه الحواسيب ، فقد تزايد عدد هذه الجرائم وتنوعت اساليبها وتعددت اتجاهاتها وزادت خسائرها وأخطارها حتى اصبحت من اخطر ما يهدد المصالح والحقوق المستقرة قانوناً ، لا سيما تلك الجرائم التي تنصب على المعلومات والبيانات (كجرائم تزوير الالكتروني) ،نظراً لأهمية ما تحويه نظم المعلومات من بيانات ، والتي قد تكون محلاً للاعتداءات عبر تغيير حقيقتها بقصد الغش في مضمونها تغييراً من شانه احداث اضرار مادية او معنوية أو أجتماعية للغير، فالتزوير يعتبر اخطر طرق الغش التي تقع في مجال المعالجة الالية للبيانات [1].

وقد تعدَّدت ألفاظ ومفردات وصِيَغ ومصطلحات التعريف بالجريمة الإلكترونية تعدُّدًا يحمل صورة التنوُّع والثراء لا التنازع والتضاد ، فأُطْلِقَ على الجريمة الإلكترونية هذا المسمَّى (E- crime) ، وجرائم الكمبيوتر والإنترنت ، وجرائم الحاسب الآلي (Computer Crimes) ، وجرائم التقنية العالية (High-Tick) ، والجرائم المعلوماتيّة (Information Crimes) ، والجرائم الرقمية (Digital Crimes) ، وجريمة أصحاب الياقات البيضاء (**White Collar**) ، والجرائم الناعمة (Soft Crimes) ، والجرائم النظيفة (Clean Crimes) [2].

وبفعل ذلك كانت الحاجة ماسة الى وجوب تطوير مراحل مكافحة الجرائم الإلكترونية "من الزاوية النظاميَّة والقانونية ، حيث تزايدت خطط مكافحة الجرائم الإلكترونية ، وانصبَّت الجهود على دراستها المتعمِّقة ، وخلق آليّات قانونيّة للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية ، خاصة المنظمات والهيئات الإقليميّة الأوروبية. وإدراكًا لقصور القوانين

---

[1] احمد حسام طه ، الجرائم الناشئة عن استخدام الحاسب الالي ، دراسة مقارنه ، دار النهضة العربية ، القاهرة ،2000، صفحة 106

[2] المحامي يونس عرب ،(دليل امن المعلومات و الخصوصية) ، الجزء الاول ، جرائم الكمبيوتر والانترنت ، اتحاد المصارف العربية ، الطبعة الاولى ، عمان ، 2002 ، صفحة 205 .

الجنائيّة بما تتضمّنه من نصوص التجريم التقليديّة عن أن تحيط بالجرائم الإلكترونية ، كان لا بد للعديد من الدول من وضع قوانين وتشريعات خاصّة ، أو العمل على جبهة قوانينها الداخلية لجهة تعديلها من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم .[3]

وفي هذا الفصل ، نقف على نشأة وتطور التزوير الالكتروني (**المبحث الاول**) ثم نتناول الاتجاهات التشريعية الدولية والوطنية لتنظيم التزوير الالكتروني (**المبحث الثاني**) .

[3] **عبد الفتاح بيومي حجازي ، جرائم الكمبيوتر و الانترنت ، دار الفكر الجامعي ، الاسكندرية ، 2002 ، صفحة 144 .**

المبحث الاول

نشأة وتطور التزوير الألكتروني

ترجع نشأة جريمة التزوير الالكتروني الى نشأة جرائم الكمبيوتر او ما كان يعرف بانشطة اساءة استخدام الكمبيوتر ، والتي ترجع فعليا الى اربعينيات وخمسينات القرن الماضي ، وبالتالي فان تتبع نشأة وتطور جريمة التزوير الالكتروني انما هو تتبع لنشأة وتطور الجرائم الالكترونية بوجه عام باعتبار التزوير الالكتروني احد ابرز صورها [4].

في هذا المبحث نتناول نشأة التزوير الالكتروني في (المطلب الاول) ، وتطور التزوير الالكتروني كاحد صور الجرائم الالكترونية في (المطلب الثاني) .

[4] **يونس عرب ، (دليل امن المعلومات و الخصوصية) ، مرجع سابق ، صفحة 209 .**

المطلب الاول

نشأة التزوير الالكتروني

نشهد حاليا ازدياد انشطة التعدي على البيانات والمعلومات المخزنة في انظمة المعلومات ، وانشطة التعدي على عمل انظمة المعلومات ذاتها ، وانشطة اساءة استخدام شبكة الانترنت ، وهي جرائم وانشطة مختلفة ، منها المستحدثة التي ولدت مع ميلاد تقنية المعلومات وتطبيقاتها المختلفة ، كجرائم الدخول غير المصرح به على انظمة المعلومات وجرائم اعتراض البيانات وتعطيل عمل الانظمة والمواقع الالكترونية وغيرها ، ومنها جرائم تقليدية استفادت من انظمة المعلومات والشبكات وحولتها الى اداة للتمكن من ارتكاب هذه الجرائم كالاحتيال الالكتروني والتزوير الالكتروني وغيرها [5].

و صور الجريمة الالكترونية او جرائم انظمة المعلومات بوجه عام هي كثيرة منها :-

1- الدخول غير المشروع النُظُم وقواعد معالجة البيانات، سواء أحدثَ هذا الدخول تلاعبًا أم لا.

2- الاعتداء على المواقع الإلكترونية سواء كان ذلك بمسح أو تعديل بيانات أو التلاعب فيها، أو إعاقة تشغيل النظام.

3-انتهاك السريَّة والخصوصيَّة للبيانات الشخصيَّة، والإضرار بصاحبها، والإطّلاع على المراسلات الإلكترونية، والإدلاء بالبيانات الكاذبة في إطار المعاملات والعمليات الإلكترونية .

4- الاعتداء على الأموال الإلكترونية -وهي الأموال المتداولة إلكترونيًّا - سواء أكان ذلك في إطار التجارة الإلكترونية أو غيرها، مثل عمليات سحب وإيداع الأموال التي تقوم بواسطة أجهزة الصراف الآلي أو الهاتف المصرفي أو الخدمات المصرفية بواسطة الإنترنت

---

5 شمس الدين ابراهيم احمد ، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، 2005 ، صفحة 5

للبنوك؛ إذْ يمكن أنْ تتعرّض هذه الأموال للسرقة والنصب وخيانة الأمانة، وذلك بواسطة بطاقات ائتمان مزورّة أو انتهت صلاحيتها أو مسروقة، أو إختراق المواقع الإلكترونية للبنوك،أو اختراق أجهزة الحاسب الآلي للبنوك أو عملاء البنوك...الخ .

5- التعدي على أموال الغير بالوسائل الإلكترونية ، مثل الدخول لمواقع البنوك والدخول لحسابات العملاء وإدخال بيانات أو مسح بيانات بغرض اختلاس الأموال أو تحويلها من حساب لآخر.

6- تزوير أو تقليد التوقيع الإلكتروني الذي هو عبارة عن رموز تميِّز صاحب هذا التوقيع، وهو بهذا المعنى يعد وسيلة تعتمد في المعاملات الإلكترونية ويقوم مقام التوقيع الكتابي [6].

وان نظام المعلومات (كما اصبح يطلق عليه بعد ربط الكمبيوترات ضمن شبكات نقل وتبادل للمعلومات) يلعب ثلاث ادوار رئيسة في نطاق الجرائم الالكترونية ، فهو قد يكون هدفها ومحلها ، وهذا يتحقق في الصور الجرمية التي تستهدف سرية وسلامة وتوفر معطيات الكمبيوتر المخزنة او المعالجة داخل نظام الكمبيوتر، كجرائم الدخول غير المصرح به الى نظم المعلومات وجرائم اتلاف المعطيات (خاصة بتقنية الفايروسات او البرامج الخبيثة) ، وجرائم تعطيل النظم وانكار الخدمات واعتراض البيانات وغيرها. وقد يكون نظام المعلومات او الكمبيوتر الوسيلة او الاداة لارتكاب الجريمة، كجرائم التزوير الالكتروني والاحتيال الالكتروني ، حيث يسخر فيها الكمبيوتر كوسيلة لارتكاب الجريمة. وقد يكون مجرد بيئة للجريمة، كسائر جرائم المحتوى الضار لمواقع المعلوماتية التي يتيح الكمبيوتر كجزء من الشبكات بيئة لمقارفة الفعل وتحقق نتائجه ، كما في مواقع ترويج المواد الاباحية او موقع انشطة القمار او غسل الاموال او الاتجار بالاسلحة او الاتجار بالبشر وغيرها من المواقع ذات المحتوى الضار في بيئة الانترنت [7].

وفي سياق هذا الوصف ، فان جريمة التزوير الالكتروني ، التي تستهدف تغيير الحقيقة في الملفات او السجلات او المستندات المعالجة الكترونيا المحفوظة لدى الغير او الخاصة بالغير او تستهدف اصطناع ملفات لا وجود لها وتغاير الحقيقة ، تنسب الى طائفة الجرائم التي يلعب الكمبيوتر فيها دور الوسيلة او الاداة التي تتيح وتسهل ارتكاب الفعل ، وان كانت مقارفتها ابتداء

[6] **يونس عرب ، (دليل امن المعلومات و الخصوصية) ، مرجع سابق ، صفحة 2011 .**
[7] **يونس عرب ، (دليل امن المعلومات و الخصوصية) ، مرجع سابق ، صفحة 2011 وما بعدها .**

تقوم باستخدام وسائل وتطبيقات تكنولوجيا المعلومات وتوجه ايضا الى معطيات مخزنة او معالجة او منقولة عبر نظم المعلومات [8].

ولخطورة جريمة التزوير الالكتروني، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (**بيانات ، ومعلومات، وبرامج بكافّة أنواعها**) ، فهي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء ، يمتلكون أدوات المعرفة التقنيةتُوَجَّه للنَّيْل مِنَ الحق في المعلومات، وتَطَال اعتداءاتها معطيات الكمبيوتر المخزّنة ، والمعلومات المنقولة عبر نُظُم وشبكات المعلومات ، وفي مقدمتها الإنترنت **[9].**

كل هذه المسائل دفعت العديد من الدول الى وضع حزمة واسعة من التشريعات لحماية هذه المعلومات من الاعتداء، او تعديل التشريعات القائمة .

وتعتبر السويد اول دولة تسن تشريعات ضد (جرائم الكمبيوتر) او ما اصبح يعرف لاحقا بالجرائم الالكترونية او جرائم المعلوماتية ، لاسيما التزوير الاكتروني ، حيث صدر قانون البيانات السويدي عام (1973) الذي عالج قضايا الدخول غير المشروع للبيانات الحاسوبية او تزويرها أو تحويلها او الحصول غير المشروع عليها، وقد صدر في بريطانيا قانون مكافحة التزوير والتزييف عام (1986) الذي شمل في تعاريفه الخاصة تعريف اداة التزوير وهي وسائط التخزين الحاسوبية المتنوعة أو أي اداة اخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الالكترونية او بأي طريقة أخرى، وفي عام 1985 سنت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الألي كالتزوير المعلوماتي. كما كانت فرنسا من الدول التي أهتمت بتطوير قوانينها للتوافق مع المستجدات الاجرامية حيث اصدرت في عام 1988 القانون رقم 19 الذي عالج التزوير المعلوماتي، أما في المانيا فقد سن المشرع الالماني قانون مكافحة التزوير المعلوماتي لسنة 1986 [10].

وهنا نجد ان جريمة التزوير الالكتروني هي من ضمن جرائم انظمة المعلومات ، وان نشاة هذه الجريمة ترتبط بنشاة الجرائم المعلوماتية و تطورها .

---

8 المحامي يونس عرب ، دليل التعريف في الجرائم الالكترونية ، اتحاد المصارف العربية ، عمان ، 2006 ، صفحة 100.
9 عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية، القاهرة 2002، صفحة 170 .
10 محمد علي العريان ، الجرائم المعلوماتية ، منشورات دار الحلبي الحقوقية ، بيروت ، 2000 ، صفحة 42 .

المطلب الثاني

تطور التزوير الالكتروني كاحد صور الجرائم الالكترونية

ان دخول تقنية المعلومات مرحلة التشبيك بين نظم الحواسيب وشبكات المعلومات ، بدأت تتخذ جرائم الكمبيوتر عموما ومن ضمنها جريمة التزوير الالكتروني اتجاها مغايرا من حيث تركز الانشطة الجرمية على توسل الدخول الى هذه الشبكات باعتبارها المدخل الى نظم الحواسيب واماكن تخزين البيانات ، وبدات الانشطة الجرمية تتجه الى استغلال التقنيات الحديثة لغرض الوصول الى المعطيات والعبث بها او الاستيلاء عليها ، وبالتالي بدأت ظاهرة جرائم الكمبيوتر تتنامي وتنشأ في ظلها جرائم جديدة والتي اطلق عليها في الاعلام جرائم الانترنت ، ولهذا يعد الانتشار الواسع للانترنت على المستوى التجاري بداية مرحلة جديدة لجرائم الكمبيوتر يمكن اعتبارها التطور الاول لها فيما اصبح يطلق عليه الجرائم الالكترونية [11].

وان التطور الجديد لتطبيقات واستخدامات تكنلوجيا المعلومات في بيئة الانترنت ، رافقه ايضا تطور في وسائل وصور التزوير الالكتروني ، حيث جرى تزايد التزوير في مجال نظم المعالجة الألية للبينات بوصفه أحد انواع الغش المعلوماتي تزايدا سريعا في السنوات الاخيرة وطالت كافة المجالات الخاصة بأدارة المنشآت العامة والخاصة ومن بينها ايضا الجهات والهيئات القضائية ، كمجال برمجة أعمال قلم كتاب المحكمة وصحف السوابق و الحالة المدنية و القوائم الانتخابية [12].

وقد تبين من خلال الرصد الميداني ان جرائم الكمبيوتر او جرائم انظمة المعلومات في تطور سريع و مستمر ،حيث بلغت **عدد الشكاوى** التي تلقّاها مركز شكاوى احتيال الإنترنت الأمريكي (IFFC) منذ بدأ اعماله في أيار (2000م) وحتى شهر تشرين ثاني من العام نفسه (أي خلال ستة أشهر فقط) (6087) شكوى ، من ضمنها (5273) حالة تتعلق باختراق الكمبيوتر عبر الإنترنت، وقد بلغت الخسائر المتصلة بهذه الشكاوى ما يقارب (4.6) مليون دولار. وأعلن مركز بلاغات جرائم الإنترنت Internet crime complain center (IC3) في تقريره السنوي لعام (2007م) أن مقدار ما تم خسارته في تكاليف الاستقبال (الاستقبال فقط) للبلاغات الناتجة من سوء

11عبد الفتاح بيومي حجازي، جرائم الكمبيوتر و الانترنت ، مرجع سابق،صفحة 199 .

12يونس عرب ، موسوعة القانون و تقنية المعلومات ، رقم 1 ، قانون الكمبيوتر ، منشورات اتحاد المصارف العربية ، عمان ، 2001 ، صفحة 111 .

استخدام الانترنت هو 198.4مليون دولار وذلك بزيادة قدرها (15.3) مليون دولار عن السنة التي قبلها [13].

وهنا يظهر انه يوجد تسارع وتطور حديث للجرائم الالكترونية او جرائم انظمة المعلومات ومنها جريمة التزوير الالكتروني ،وهو نيجة حتمية لثورة المعلومات او ان صح التعبير الانفجار المعلوماتي .

الا ان هذا التطور الهائل حمل معه مزيدا من المخاطر الاقتصادية والامنية والاخلاقية والاجتماعية على العالم اجمع .

فمن حيث "الفاتورة" الإجمالية لجرائم أمن المعلوماتعالميًّا وعربيًّا في (**2011م**)، فانها تُقدَّر وحدها بحوالي (388) مليار دولار أميركي ، أما التكلفة النقدية المباشرة لهذه الجرائم المتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجمات فتقدر بحوالي (114) مليار دولار، ومعنى ذلك أنَّ القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات الماريجوانا والكوكايين والهيروين مجتمعين التى تقدر بحوالى (288) مليار دولار، وتزيد عن قيمة السوق العالمية للمخدرات عموما التى تصل إلى (411) مليار دولار، وأعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة (اليونيسيف) بحوالى 100 ضعف، حيث تصل ميزانيتها إلى (3.65) مليار دولار، كما تعادل هذه الخسائر ما تم إنفاقه خلال 90عامًا على مكافحة الملاريا وضعف ما تم إنفاقه على التعليم في 38 عاما. وقد بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم 50 ألف جريمة واعتداء في الساعة، تأثَّر بها (589) مليون شخص، وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوروبا مجتمعين، ويعادل 9% من إجمالى سكان العالم. وقد توزَّعت هذه الجرائم ما بين جرائم الفيروسات والبريد الإلكتروني الملوث والضار، وجرائم الاحتيال والتزوير والاصطياد (الحصول على معلومات بنكية سرية)، والجرائم المتعلقة باختراق الهواتف المحمولة [14].

وأمَّا الخطورة الأخلاقية فإنَّ جلّ جرائم الإنترنت تستهدف فضح الأسرار الشخصيّة أو القذف أو التشهير بشركات أو أشخاص بقصد الإضرار بالسمعة الشخصية أو المالية ، إمّا بسبب المنافسة ، أو بداعي الانتقام ، ونحو ذلك. وأيضًا على شبكة الإنترنت تنشط تجارة الدعارة والصور الخليعة التي تُعدّ أكبر صناعة نشطة على شبكة الإنترنت بحجم عائدات كبير يُقَدَّر بنسبة 58% من مجمل عائدات الخدمات المدفوعة على الشبكة لعام (2003م)وعبر آلاف المواقع تُنشَر صور

13المحامي يونس عرب ، المدخل الى الجرائم المعلوماتية ، (جرائم الكمبيوتر) ، دار النهضة العربية ، القاهرة ، 2009 ، صفحة ، صفحة 116 .

14محمد محي الدين عوض،مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)،ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي،القاهرة ،25-28 تشرين اول 1993 ، صفحة 32 .

فاحشة، وتُقَدَّم خدمات جنسيّة مدفوعة، وتُستغل صور الأطفال والمشاهير في أوضاع شائنة، دون أن تنال كثيرًا من هذه الأنشطة يد القوانين المحليّة أو الدولية [15].

وأمَّا الخطورة الأمنية والمجتمعيَّة فقد لا يُدرك كثيرون أنّ الجماعات المتطرّفة كانت من أوائل الجماعات الفكريّة التي دخلت العالم الإلكتروني حتى قبل أنْ تظهر شبكة الإنترنت بسنوات. وممّا تشير إليه المصادر الغربيّة أنَّ «توم ميتزقر» (Tom Metzger) أحد أشهر المتطرّفين الأمريكيّين العنصريّين (اليمين المتطرّف) ومؤسّس مجموعة المقاومة «الإريانية البيضاء» (White Aryan Resistance) كانمِن أوائلمَن أسّس مجموعة بريد إلكترونيّة ليتواصل مع أتباعهويبثّ أفكاره سنة (1985م). ومما غاب عن بعض الباحثين أنَّ المجموعات البريدية الإلكترونية كانت الأكثر توظيفًا مِن قِبل الجماعات العِرقيّة المتطرّفة قبل ظهور الإنترنت التجاري، وربما ظلت على هذا النمط حتى ما بعد منتصف التسعينيات. وقد عُرفت جماعات كثيرة عبر شبكات المعلومات ما قبل الإنترنت مثل مجموعة المتطرف الأمريكي «دان جانوون» (Dan Gannon) الذي يعد بحسب المصادر الغربية أول من أنشأ موقعًا متطرِّفًا يَبثّ من خلاله أفكاره العُنصريّة عن نقاء العرق الأبيض في شهر ديسمبر (1991م) مع ولادة الإنترنت في الولايات المتحدة. وتلى ذلك عدة مجموعات اشتهر منها بعد ذلك مجموعة «جبهة العاصفة» (Stormfront) الأمريكية المسيحية المتطرفة بقيادة «دون بالك» (Don Black) التي أنشأت أول موقع متكامل عن التطرُّف وثقافة الكراهية في مارس سنة (1995م). وقد تتالى ظهور مواقع تابعة لجماعات متطرِّفة من الولايات المتحدة وأوروبا وبشكل خاص بريطانيا وأستراليا، ثم بقية دول العالم. وفي كل هذه المراحل كان الإنترنت في عمق دائرة ترويج ثقافة التطرُّف والعنف، معبِّرة عن أفكار المهمَّشين والمتطرِّفين الصاخبين من كل ملة وجنس [16].

والمتابع للجرائم الالكترونية ، يجد اخبارا وتقارير شبه يومية تصنف الجرائم الالكترونية الاكثر شيوعا ، فتحتل جرائم الاحتيال الالكتروني التي تستهدف الاستيلاء على الاموال والتعدي على الحقوق المالية راس قائمة الجرائم الالكترونية الاكثر شيوعا ، تليها جرائم التعرض للكرامة والسمعة والمساس بالافراد خاصة جرائم شبكات التواصل (الفيس بوك مثلا) ، وجرائم القرصنة التي تستهدف حقوق الملكية الفكرية على المصنفات الرقمية والالكترونية ، ثم **جرائم التزوير الالكتروني** بانواعها (خاصة تلك الضرورية لتنفيذ انشطة الاحتيال المالي الالكتروني) ، و هي موضوع ومادة هذه الرسالة .

---

15 محمد محي الدين عوض،مرجع سابق، صفحة 33 .
16 محمد محي الدين عوض ، مرجع سابق، صفحة 34 .

المبحث الثاني

الاتجاهات التشريعية الدولية والوطنية لتنظيم التزوير الالكتروني

لقد كان من الضروري أن تواكب التشريعات المختلفة التطور الملحوظ في جرائم التزوير الالكتروني، وذلك من خلال نظم قانونية غير تقليدية لهذا الإجرام غير التقليدي، وان تتعامل هذه المواجهة التشريعية بشكل عصري ومتقدم مع الجرائم الالكترونية المختلفة، التي يأتي في مقدمتها الدخول غير المشروع على شبكات الحاسوب ونظم المعلومات، والتحايل على نظم المعالجة الآلية للبيانات ونشر الفيروسات وإتلاف البرامج وتزوير المستندات، ومهاجمة المراكز المالية والبنوك وتعديها إلى الحروب الإلكترونية، والإرهاب الإلكتروني، ونشر الشائعات والنيل من هيبة الدول، إضافة إلى نشر الرذيلة والإباحية وغيرها من الجرائم الإلكترونية، وقد لفتت بالفعل هذه الأعمال الإجراميّة أنظار الدول والهيئات الدولية التي أدركت خطورتها وسهولة ارتكابها وتأثيرها المباشر؛ لتجعل مكافحتها من أولى أولويات المجتمع الدولي والحكومات، ما حتّم أهمية الحماية القانونية لمواجهة هذه الأفعال الإجرامية [17].

وقدأظهر تحليل الجهود الدولية ، واتجاهات القانون المقارن بشأن جرائم الكمبيوتر والإنترنت أنّ مواجهة هذه الجرائم تم في ثلاثة قطاعات مستقلة :-

1- حماية استخدام الكمبيوتر، أو ما يُعرَف أحيانًا بجرائم الكمبيوتر ذات المحتوى الاقتصادي.
2- حماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية) .
3- حماية حق المؤلف على البرامج وقواعد البيانات (الملكية الفكرية للمصنفات الرقمية [18].

ومن هنا تزايدت خطط مكافحة الجرائم الإلكترونية، وانصبَّت الجهود على دراستها المتعمِّقة، وخلق آليّات قانونيّة للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية، خاصة المنظمات والهيئات الإقليميّة الأوروبية. وإدراكًا لقصور القوانين الجنائيّة بما تتضمّنه من نصوص التجريم التقليديّة عن أن تحيط بالجرائم الإلكترونية ، كان لا بد للعديد من

17سامي الشوا ، جرائم الحاسب الالي والجرائم الاخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال (الانترنت)، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي،25-28 تشرين الاول 1993 ، صفحة 16 .

18 سامي الشواء ، جرائم الحاسب الالي و الجرائم الاخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال (الانترنت)، مرجع سابق ، صفحة 17 .

الدول من وضع قوانين وتشريعات خاصّة، أو العمل على جبهة قوانينها الداخلية لجهة تعديلها من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم [19].

وقد تبلور هذا الاهتمام من خلال بروز العديد من القوانين الدولية والعربية في مكافحة الجريمة الإلكترونية وذلك من خلال سن قوانين و تشريعات تنظم العمل بهذا الحقل وتوفر الحماية القانونية للمعلومات و نظمها المختلفة ومن هذه الدول [20] :-

1- قانون البيانات السويدي عام (1973م) و تعتبر السويد أول دولة تسن تشريعات ضد جرائم الإنترنت أو جرائم المعلوماتية، لا سيَّما التزوير المعلوماتي؛ حيث صدر قانون البيانات السويدي عام (1973) الذي عالج قضايا الدخول غير المشروع للبيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها.
2- قانون مكافحة جرائم الحاسب الآلي والانترنت الدنماركي (1985م) ، وفي عام 1985 سنَّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت التي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الألي كالتزوير المعلوماتي .
3- القانون الفرنسي الخاص بالتزوير المعلوماتي (1988م) ، أصدرت فرنسا في عام (1988م) القانون رقم 19 الخاص بالتصدِّي للتزوير المعلوماتي .
4- اتفاقية الإجرام السيبيري (الإجرام عبر الانترنت) (2001م) ، صدرت هذه الاتفاقية عن المجلس الأروبي، ووُقِّعَت في العاصمة المجرية بودابست في 23 نوفمبر (2001م)، وقّعت عليها 30 دولة ولأهمية هذه الاتفاقية انضمَّ إليها العديد من الدول من خارج المجلس الأوروبي، وأبرز هذه الدول الولايات المتحدة الأمريكية ، التي صادقت عليها في 22 سبتمبر (2006) ، ودخلت حيز النفاذ في الأول من يناير (2007م) ، واشتملت على عدة جوانب من جرائم الإنترنت ، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال .
5- قانون مكافحة الجرائم الإلكترونية (مواده مستحدثة ضمن أحكام قانون الجزاء العماني) ، بسلطنةعُمَان (2001م) ، أصدرت سلطنة عمان جملة من التشريعات لمكافحة الجريمة المعلوماتية تحت مسمى (قانون سلطنة عمان لمكافحة جرائم الحاسب الآلي) ، فقد صدر المرسوم السلطاني رقم (72) لسنة (2001 م) بشأن تعديل بعض أحكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي (الكمبيوتر) ، وذلك بإضافة فصل في الباب

19واثبة داود السعدي ،المعالجة الدولية والوطنية لجرائم الحاسب الالي ، دراسة مقارنة في جرائم تكنولوجيا المعلومات ونظمها المختلفة، ، بدون دار نشر ، بغداد ، 2004 ، صفحة 118.
20واثبة داود السعدي ، المعالجة الدولية والوطنية لجرائم الحاسب الالي ، مرجع سابق ، صفحة 118.

السابع من قانون الجزاء العماني تحت عنوان (جرائم الحاسب الآلي) ، وكذلك أضيفت مواد إلى قانون الاتصالات العماني تحرم تبادل رسائل تخدش الحياء العام وتحرم استخدام أجهزة الاتصالات للإهانة أو الحصول على معلومات سرية أو إفشاء الأسرار أو إرسال رسائل تهديد ، وأسست السلطنة قانوناً ينظم المعاملات الحكومية الإلكترونية والتوقيع الإلكتروني وحوادث اختراق الأنظمة .

وسوف نتناول في هذا المبحث الجهد الدولي التشريعي للتصدي للجرائم الالكترونية ومن ضمنها التزوير الالكتروني (**المطلب الاول**) ، ثم نقف على الاتجاهات وابرز ملامح الجهود الوطنية في ذات الحقل في (**المطلب الثاني**) .

المطلب الاول

الاتجاهات الدولية لتنظيم التزوير الالكتروني

ان التصدي للجرائم التزوير الالكتروني على الصعيد الدولي ، متمثلا بجهد الامم المتحدة ، انطلق ضمن اعمال المؤتمرات الدولية لمكافحة الجريمة ، حيث ظهر وتبلور هذا الاهتمام بشكل فعلي في المؤتمر الثامن للأمم المتحدة لمنع الجريمة ومعاملة المجرمين المنعقد في هافانا- كوبا (27 أيلول - 7 تشرين أول 1990) حيث صدر عن هذا المؤتمر قرار خاص بالجرائم ذات الصلة بالكمبيوتر [21].

وقد كانت حصيلة اعمال هذا المؤتمر فيما يتصل بجرائم الكمبيوتر ، صدور القرار رقم (7) المعنون بـ (الجرائم ذات الصلة بالكمبيوتر ، Computer-ralated crimes) ، والذي أكد على أن "نظم الكمبيوتر تستخدم بشكل شائع لتخزين بيانات سياسية واقتصادية وطبية واجتماعية وشخصية تتسم بحساسية بالغة قد تستخدم لأداء ومراقبة مهام معقدة كثيرا ما تنطوي على حالات قد تعرض للخطر الحياة وحقوق الانسان والحريات الأساسية "وأن زيادة استخدام تكنولوجيا الكمبيوتر وشبكات الاتصالات السلكية واللاسلكية عن طريق الكمبيوتر تهئ ظروفا تسهل الى حد كبير ارتكاب العمليات الاجرامية داخل البلدان وفيما بينها" [22].

وقد اوصى هذا المؤتمر بان تتضمن قائمة الحد الادنى للافعال المتعين تجريمها واعتبارها من قبيل جرائم الكمبيوتر ما يلي :-

1- الاحتيال او الغش المرتبط بالكمبيوتر **:-** ويشمل الادخال والاتلاف والمحو لمعطيات الكمبيوتر او برامجه ، او القيام باية افعال تؤثر بمجرى المعالجة الالية للبيانات وتؤدي الى الحاق الخسارة او فقدان الحيازة او ضياع ملكية شخص وذلك بقصد جني الفاعل منافع اقتصادية له او للغير .

---

21 لمحامي عادل امين ، المؤتمر الثامن للأمم المتحدة لمنع الجريمة ومعاملة السجناء (الواقع والقرارات) ، الطبعة الاولى ، اتحاد المحامين العرب ، القاهرة، 1991، صفحة 37 .

22 المحامي عادل امين ،مرجع سابق، صفحة 40 .

2- التزوير المعلوماتي :- ويشمل ادخال او اتلاف او محو او تحوير المعطيات او البرامج او اية افعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكمبيوتر وتعد – فيما لو ارتكبت بغير هذه الطرق – من قبيل افعال التزوير المنصوص عليها في القانون الوطني.

3- الاضرار بالبيانات والبرامج (الاتلاف) :- وتشمل المحو والاتلاف والتعطيل والتخريب لمعطيات الكمبيوتر وبرامجه .

4- تخريب واتلاف الكمبيوتر :- وتشمل الادخال او المحو او الاتلاف او التخريب او اي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر او نظام الاتصالات (الشبكات) .

5- الدخول غير المصرح به ، وهو التوصل او الولوج دون تصريح الى نظام او مجموعة نظم عن طريق انتهاك اجراءات الامن .

6- الاعتراض غير المصرح به ، وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر او عدة نظم او شبكة اتصالات [23].

كما ان هيئة الامم المتحدة ، وتحديدا عبر لجان مناطقها الاقتصادية والاجتماعية المتخصصة، حرصت على مساعدة مختلف دول العالم في ميدان سن التشريعات المتصلة بالجرائم الالكترونية ، بل التشريعات ذات العلاقة بتنظيم البيئة الرقمية والتي تشمل تشريعات الجرائم الالكترونية ، وتشريعات حماية الخصوصية (حماية البيانات الشخصية لمستخدمي التقنية) ، وتشريعات التجارة والاعمال الالكترونية ، وتشريعات المعايير والمقاييس الخاصة بالخدمات الالكترونية ، وتشريعات الاعلام الالكتروني ، وتشريعات حماية الملكية الفكرية في البيئة الرقمية، وتشريعات تنظيم خدمات الاتصالات وتكنولوجيا المعلومات والهيئات المشرفة عليها في الدولة ، وغيرها من التشريعات . وفي هذا السياق وبالنسبة للدول العربية ، مثلت تجربة اللجنة الاقتصادية الاجتماعية لغرب اسيا (الاسكوا) وجهودها منذ العام 2007 تجربة رائدة في دعم الجهود التشريعية العربية وفي تبيان الاحتياجات التشريعية المطلوبة للتصدي لمسائل البيئة الرقمية ومنها الجرائم الالكترونية ، حيث وضعت في العام 2007 ما سمي (نماذج تشريعات الفضاء السيبراني) ،

23 المحامي عادل امين ، مرجع سابق ، صفحة 43 .

واعقبها في العام 2008 وضع دراسة مسحية لواقع التشريعات العربية في كافة فروع وحقول البيئة الرقمية ومنها الجرائم الالكترونية ، واستكملت هذه الدراسات في لعام 2010 لجهة بين التطورات التي لحقت في جميع الدول العربية منذ الدراسة الاخيرة في العام 2008 ، وبعدها شرعت (الاسكوا) بتقديم مشاريع القوانين والدراسات المسحية والاستشارات التشريعية للدول العربية ، وانجزت للان مساعدة فعلية في وضع تشريعات تكنولوجيا المعلومات او تعديلها لكل من الاردن ، وسوريا ، ولبنان ، وفلسطين ، وسلطنة عمان ، والبحرين ، وقطر ، واليمن ، وغيرها [24].

اما التدبير التشريعي الوحيد القائم على الصعيد الدولي في حقل التزوير الالكتروني (كاحدى الجرائم الالكترونية) هو اتفاقية بودابست الخاصة بالجرائم الالكترونية للعام 2001 ، حيث نصت المادة (7) من هذه الاتفاقية وتحت عنوان التزوير المرتبط بالكمبيوتر ، على ما يلي :-

((تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير اخرى لتجريم الافعال التالية في قانونها الوطني ، اذا ما ارتكبت عمدا ، وبغير حق :-

ادخال ، او تبديل او محو ، او تدمير معطيات كمبيوتر ، ينتج عنها معطيات غير اصلية بقصد استخدامها او التعويل عليها في اغراض قانونية كما لو كانت اصلية ، بغض النظر عما اذا كانت هذه المعطيات مقروءة ومفهومة بشكل مباشر من عدمه ، ويجوز لطرف ان يشترط وجود نية الغش (التدليس) او وجود قصد غير امين مشابه (سوء النية) لقيام المسؤولية الجزائية)) [25].

وهنا نجد ان النص الدولي المتقدم قد تناول بالتفصيل ما يلي من الحقائق :-

1) من حيث محل الجريمة اشار النص الى معطيات الكمبيوتر ، سواء اكانت تدرك بالبصر ام لا ، وهو ما عبرت عنه عبارة (بغض النظر عما اذا كانت هذه المعطيات مقروءة ومفهومة بشكل مباشر من عدمه) ، ومعطيات الكمبيوتر مصطلح واسع النطاق يشمل البيانات ، والمعلومات المعالجة باشكال ملفاتها المختلفة كالوثيقة والسجل والرسالة وغيرها .
2) من حيث السلوك الجرمي لجريمة التزوير الالكتروني ، فان الافعال تتمثل بالاصطناع ابتداء او بالاضافة (ادخال) ، والتغيير او الاستبدال ، والمحو او الاتلاف او تدمير المعطيات .

24 المحامي يونس عرب ، بناء الثقة في البيئة الرقمية في الدول العربية ، دراسة مسحية للتشريعات السيبرانية ، منشورات منظمة الاسكوا لدول غرب اسيا ، بيروت ،2010، صفحة 33 .

25نص المادة 7 من اتفاقية بودابست الخاصة بالجرائم الالكترونية للعام 2001.

3) النتيجة الجرمية للافعال الجرمية هي انتاج معطيات يعول عليها وتبدو كانها بيانات اصلية.

4) تحتاج الجريمة قصدا خاصا هو نية استخدام هذه المعطيات لاغراض مشروعة وقد استخدم النص عبارة (بقصد استخدامها او التعويل عليها في اغراض قانونية) .

5) اتاح النص للمشرعين الوطنيين اضافة قصد غير نية الاستعمال او الاستخدام، فجاء فيه (للطرف ان يشترط وجود نية الغش (التدليس) او وجود قصد غير امين مشابه (سوء النية) لقيام المسؤولية الجزائية)) وبالتالي قد يشترط النص سوء النية وقد يشترط غير ذلك.

6) كما لا يمنع النص المشرع من اشتراط حصول الضرر ، وعندها يكون اشتراط حصول الضرر عنصرا في الركن المادي او يمكن ان نعتبره ركنا مستقلا [26].

هذا عرض للتدابير التشريعية الدولية ، وثمة تدابير تشريعية اقليمية ، وحهود لهيئات ومنظمات دولية ، ومؤسسات اكاديمية متخصصة ، لا يتسع المقام لاستعراضها ، محيلين القاريء الكريم الى المراجع المتخصصة التي تناولتها تفصيلا .

26 يونس عرب ، التزوير والاحتيال المالي – الأطر التطبيقية والعلمية و المستجدات الفنية في ظل التطور التكنولوجي ، ورقة عمل مقدمة الى دورة التزوير والاحتيال الالكتروني التي عقدتها مؤسسة الاستشارية لادارة المخاطر و المركز العربي للقانون والتقنية العالية بالتعاون مع شركة كيسنغ الهولندية للنظم المرجعية ، جمعية البنوك في الاردن ، 2004/7/7 ، صفحة 6 .

المطلب الثاني

الاتجاهات الوطنية لتنظيم التزوير الالكتروني

شهدت ثمانينيات وتسعينات القرن المنصرم ، موجة تشريعية واسعة على الصعد الوطنية في حقل الجرائم الالكترونية تناولت من ضمن ما تناولت جريمة التزوير الالكتروني تحت مسميات عديدة اخرى منها التزوير المعلوماتي او تزوير المستندات الالكترونية وغيرها ، وامتدت هذه التدابير التشريعية الى مختلف النظم القانونية ، حيث شهدت اوروبا بوجه عام سن قوانين الجرائم الالكترونية ، وكذلك الحال في امريكا على مستوى الولايات والمستوى الفدرالي ، وكندا واستراليا واليابان وعدد كبير من دول شرق اسيا ، وتعمق هذا الجهد واتسع ليمتد الى دول اوروبا الشرقية مع تدخل هيئات الاتحاد الاوروبي (مجلس اوروبا والبرلمان الاوروبي) لوضع ادلة ارشادية تطورت لاحقا الى اتفاقية دولية اوروبية هي **اتفاقية بودابست بشان الجرائم الالكترونية** (جرائم السايبر) لعام 2001 ، التي استعرضنا في المطلب الاول ما تضمنته بشان التزوير الالكتروني[27] .

وتتباين التشريعات الوطنية المقارنة في النص على جريمة التزوير الالكتروني ، ويمكن القول في هذه المرحلة ، وبايجاز ، ان جميع دول اوروبا ، وكذلك امريكا الشمالية على المستويات الولائية والفدرالية ، وغالبية دول امريكا الجنوبية ، والمكسيك واستراليا وكندا ونيوزلندا واليابان والصين وتايوان وتايلند وماليزيا ، وجنوب افريقيا وعدد من الدول الافريقية الاخرى ، قد وضعت تشريعات في ميدان الجرائم الالكترونية وتضمنت جميعها نصوصا تجرم التزوير بواسطة الكمبيوتر ، وقد اتجهت من حيث مضمون النص على تجريم كل سلوك يستهدف تغيير الحقيقة (اما في معطيات الكمبيوتر عدا البرامج وفقا لمنهج التوسع في نطاق التزوير ، او في المستند المعالج الكترونيا وفقا لمنهج تضييق نطاق التزوير وتمييزه عن جريمة العبث بالمعطيات لغرض غير التزوير) ، وجميعها نصت على قصد استعمال المعطيات المزورة او المستند المزور في غرض يحقق منافع او يلحق ضررا بالغير او ليكون مقبولا بصورة قانونية[28] .

واما على صعيد الدول العربية (الاسيوية والافريقية) ، فقد اظهرت الدراسات المسحية والمتخصصة التي اجرتها منظمة الاسكوا للاعوام 2007 و 2008 و 2010 النتائج التاليه :-

---

27 يونس عرب ، الاطار القانوني للارهاب الالكتروني واستخدام الانترنت للاغراض الارهابية ، ورقة عمل مقدمة الى مؤتمر تمويل الارهاب في بيئة الانترنت ، تنظيم جامعة نايف العربية للعلوم الامنية وجامعة القاهرة ، منعقد في جامعة القاهرة ، من 25-27 تشرين اول 2010، صفحة 25 .

28 يونس عرب ، الاطار القانوني للارهاب الالكتروني واستخدام الانترنت للاغراض الارهابية ، مرجع سابق ، صفحة 25 .

1- الدول العربية التي وضعت تشريعات خاصة بجرائم الكمبيوتر من الناحية الموضوعية (نصوص التجريم) هي الامارات العربية المتحدة ، والسعودية (نظام الجرائم المعلوماتية) ، وقطر ، وسلطنة عمان ، وتونس ، والمغرب ، والجزائر والسودان، وسوريا، والاردن من خلال قانونه الاخير (القانون لمؤقت المتعلق بجرائم انظمة المعلومات المقر في يلول 2010 وسبقه نص عام في قانون المعاملات الالكترونية لعام 2001) . وثمة مشاريع قانونية لم تقر بعد في كل من مصر وليبيا ولبنان وفلسطين والعراق والكويت والبحرين واليمن . وليس ثمة اي جهود في الصومال وجيبوتي وموريتانيا وجزر القمر .

2- القوانين العربية للجرائم الالكترونية جاءت قاصرة بوجه عام ، صحيح ان بعضها تضمن تجريم غالبية صور استغلال نظم المعلومات والانترنت غير انها في الغالب جاءت قاصرة عن الاحاطة بمختلف صور الجرائم الالكترونية مع تميز في قوانين سلطنة عمان وسوريا السودان ، وجاءت جميع قوانين الدول العربية (عدا القانونين السوري ونسبيا النظام السعودي) قاصرة اكثر في الاحاطة بالقواعد الاجرائية الملائمة لهذه الجرائم .

3- بخصوص التزوير الالكتروني ، فان جميع التشريعات العربية التي جرى سنها في حقل الجرائم الالكترونية نصت على تجريم الدخول غير المصرح به الى انظمة المعلومات والقيام باحداث اي تغيير في البيانات ، بمعنى جرمت العبث بالبيانات ايا كان شكلها ، وفقط اربع تشريعات عربية هي التي جرمت التزوير الالكتروني الى جانب جريمة العبث بالبيانات ، واشترطت للتزوير الالكتروني اركانا وعناصر خاصة ، وهي تشريعات كل من سلطنة عمان ، تونس ، والسودان ، وسوريا .

4- نصت تشريعات المعاملات الالكترونية في الاردن ودبي والبحرين وسلطنة عمان على تجريم بعض صور الجرائم في البيئة الرقمية لكن ايها لا يعد تشريعا شموليا كافيا لتغطية هذا الحقل من حقول قانون تقنية المعلومات ، ويعد ما سمي بالنص الاحتياطي في هذه التشريعات (كالمادة 38 من قانون المعاملات الالكترونية الاردني) والذي جرم ارتكاب اية جريمة تقليدية بوسيلة الكترونية ، نصا غير متفق مع النصوص الجزائية التي تقوم على وجوب ايراد السلوك المادي وعناصر الجريمة وتحديد العقوبة ، وهذا النص لا يزال يواجه بقاعدة حظر القياس في النصوص الجزائية .

5- ثمة تنظيم متقدم لدى بعض الدول العربية بشان ما يعرف بالسلامة المعلوماتية او مراكز التدخل او طواريء المعلوماتية (فرق السيرت CERT) ، وهي الجهة التي تتصدى لرصد الاختراقات وتتبع مصدرها ، وابرز مثال على ذلك تونس – من حيث التنظيم القانوني وايجاد الجهاز التقني لذلك ، والسعودية ومصر والامارات وسلطنة عمان وقطر – من حيث ايجاد فرق التحري والمراقبة والتدخل - ، في حين ثمة بدايات عمل وخطط لم تستكمل بهذا الاتجاه لدى بقية لدول كالكويت والاردن وغيرها .

6- لم تتدخل أي من الدول العربية لتطوير تشريعات الاجراءات الجنائية بما يتناسب مع الجرائم الالكترونية وتحدياتها في ميدان ضبط الادلة والتفتيش والاختصاص وغيرها من المسائل الاجرائية الناشئة عن هذه الانماط الجديدة من الجرائم ، رغم ان غالبية الدول العربية افردت اقساما خاصة ضمن اجهزة الضابطة العدلية او الضابطة القضائية (الاجهزة الشرطية) لجهة تولي انشطة الاستدلال بشان الجرائم الالكترونية ، لكن التجارب متفاوتة من حيث فعاليتها وجديتها وتميزها، ويظل وجه القصور الرئيس في انعدام وجود و/او عدم شمولية وفعالية الموجود من مختبرات الدليل الرقمي .

7- تحققت كثير من برامج التدريب والتاهيل في الدول العربية في ميدان الامن والاجرام المعلوماتي (اكثرها تحقق في منطقة الاسكوا) لكن مخرجاتها ليست كافية بالنظر لعدم مؤسسية هذه البرامج ، وبالنظر لغياب البعد التطبيقي العملي عن غالبيتها ، وللشعور العام لدى المتدربين بعدم فعالية محتواها بالنظر لغياب مرجعيات العمل وفي مقدمتها الادوات التشريعية التي تحسم الجدل النظري حول هذا الموضوع ، واخيرا بسبب عدم الانفاذ العملي لتوصيات ورش العمل والانشطة العلمية والتدريبية [29].

29 المحامي يونس عرب ، الاطار القانوني للارهاب الالكتروني واستخدام الانترنت للاغراض الارهابية ، ورقة عمل مقدمة الى مؤتمر تمويل الارهاب في بيئة الانترنت ، مرجع سابق ، صفحة 28 وما بعدها .

الفصل الاول

ماهية التزوير الالكتروني

تمهيد وتقسيم :-

ان ماهية التزويرالالكتروني او المعلوماتي تستلزم تعريف التزوير بوجه عام ومن ثم التزوير الالكتروني بشكل خاص ، وذلك كنقطة انطلاقة لتحديد مفهوم هذه الجريمة ،وتستلزم كذلك معرفة محل جريمة التزوير الالكتروني باعتبار ان محل هذه الجريمة يختلف عنه في جريمة التزوير العادية او التقليدية ، وبيان صور جريمة التزير الالكتروني في حال ان كان لها اكثر من صورة ، ومدى انطباق نصوص التزوير العادية على هذه الصورالجديدة .

لذلك سنقسم هذا الفصل الى مبحثين نتناول في المبحث الاول تعريف ومحل جريمة التزوير الالكتروني ، فنتناول في المطلب الاول تعريف التزوير الالكتروني ، ونتناول في الثاني محل هذه الجريمة ، ومن ثم نتناول في المبحث الثاني صور جريمة التزوير الالكتروني، حيث نقسم هذا المبحث الى مطلبين الاول صور التزوير الالكتروني بالنظر الى محل الجريمة ، والثاني صور التزوير الالكتروني بالنظر الى طريقة ارتكاب الفعل .

المبحث الاول

تعريف ومحل التزوير الالكتروني

لا بد لتعريف التزوير الالكتروني ان يتم تعريف التزوير التقليدي بوجه عام ، وذلك حتى يتسنى التميز بين جريمة التزوير التقلدية وبين جريمة التزوير الالكتروني ، ومن جه اخرى ان الوقوف على التعريف الدقيق لجريمة التزوير الالكتروني يستلزم في الضرورة البحث في محل جريمة التزوير الالكتروني – موضوع الجريمة - مع الاخذ بعين الاعتبار محل جريمة التزوير العادية او التقلدية عند اجراء المقارنه .

وعليه سوف نخصص المطلب الاول لتعريف التزوير الالكتروني ، و نخصص المطلب الثاني لمعرفة محل جريمة التزوير الالكتروني و مقارنتها بمحل جريمة التزوير التقلدية متى امكن ذلك .

المطلب الاول

تعريف التزوير الالكتروني

التزوير لغة : اصلاح الكلام وتهيئته ,وكلمة التزوير مشتقة من الزور وتعني الكذب والباطل فيقال كلام مزور ومموه بالكذب ,والتزوير اذا "اصلاح الكذب" [30].

اما التزوير (forgery) اصطلاحا : فيعرف بشكل عام بأنه ، "تغيير الحقيقة ايا كانت وسيلته وايا كان موضوعه " [31]. وان هذا التعريف يتسع للعديد من الجرائم التي نصت عليها قوانين العقوبات ، كتزوير البنكنوت (العملة) ، وتزوير الاختام وتزوير الطوابع وغيرها .

اما التزوير في الاسناد او المحررات ، فهو حسب التعريف المستقر في الفقهين الفرنسي والمصري " تغيير الحقيقة في محرر باحدى الطرق التي نص عليها القانون، تغييرا من شأنه احداث ضرر مقترن بنية استعمال المحرر المزور فيما اعد له" [32].

وقد عرفت المادة 260 من قانون العقوبات الاردني التزوير بأنه " تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد اثباتها بصك او مخطوط يحتج بهما نجم او يمكن ان ينجم عنه ضرر مادي او اجتماعي" [33].

اما التزوير في الفقه الجنائي فهو تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر اخر باحدى الطرق المادية او المعنوية التي يبينها القانون، تغييراً من شانه احداث ضرراً بالمصلحة العامة أو مصلحة شخص من الاشخاص [34].

وبالرجوع الى قوانين العقوبات العربية ، نجدها في معرض تجريم التزوير عموما ، وتزوير المحررات على وجه الخصوص قد نصت على تجريم العديد من الصور، فقد نص قانون العقوبات الاردني ـ على سبيل المثال ـ على هذه الجرائم في الفصل الثاني من الباب الخامس تحت عنوان الجرائم المخلة بالثقة العامة (المواد 260-272) ، وساوى في العقوبة بين مرتكب جريمة

---

30 ابن منظور (ابو الفضل جمال الدين محمد ابن مكرم) ، لسان العرب ، طبعة 1 ، جزء 6 ، منشورات دار صادر ، بيروت ، 1968 ، صفحة 164 .

31 محمود نجيب حسني ، شرح قانون لعقوبات – القسم الخاص ، بدون رقم طبعة ، دار النهضة العربية ، القاهرة 1992 ، صفحة 192 .

32 محمود نجيب حسني ، شرح قانون لعقوبات – القسم الخاص ، مرجع سابق ، صفحة 215.

33 قانون العقوبات الاردني رقم 16 لسنه .

34 فوزية عبد الستار ، شرح قانون العقوبات – القسم الخاص ، دار النهضة العربية ، الطبعة الثالثة ، القاهرة ، 1990 ، صفحة 215 .

التزوير و مستعمل المحرر المزور، وكذلك فان قانون العقوبات المصري نظم جرائم التزوير في الباب السادس عشر من الكتاب الثاني تحت عنوان التزوير (المواد 206-227) [35].

ويهمنا في هذا المقام الاشارة الى ان المشرع الصري قد جرم استعمال المحررات المزورة ، لكنه نهج نهج مختلف عن المشرع الاردني بشأن العقوبات ، اذ تتعدد العقوبات فيما بين جرائم تزوير المحررات تبعا لنوع المحرر محل التزوير ، وتتباين عن عقوبات جرائم استعمال المحررات المزورة كما انها تتباين في الطائفة الاخيرة [36].

وبذلك فأن التزوير يختلف عن الصورية من حيث انها لا تعد تزويراً على الرغم من انها تنطوي على تغيير في حقيقة بعض شروط العقد وذلك لأن المتعاقدان لم يتصرفا في مال الغير او حقوقه او صفاته وانما تصرفا في حق من حقهما وبالتالي فأن هذا التغيير لايحدث ضرراً بالغير، إلا إذا مس مركز الغير وحقوقه وإن من شأن هذا المساس الاضرار بالمصلحة العامة او بشخص من الاشخاص [37].

كماأن الاقرارات الفردية لاتعد صورة من صور التزوير ايضاً على اعتبار ان الأضرار يخص المقر وحده دون غيره إذ ليس من شانه أن يعكس المقر حقاً او يجعل له سنداً ويشترط فيه أن لا يكذب واقع الحال لاسيما في المحررات الرسمية لأنه إذا كان غير مطابق للحق فاعله على التزوير في حالات رسمية من قبيل هذه الاقرارات ما يحصل في سجلات المواليد والوفيات والزواج والطلاق [38].

كذلك فأن التزوير يقترب من الاحتيال لأنهما يتفقان في الكذب والباس أمور على غير حقيقتها ثوب الحقيقة اي انهما يتفقان من حيث قيامهما على تغير الحقيقة ،و لكنهما يختلفان اختلافاُ جوهرياً في ان التزوير يشترط وقوعه على محرر اما الاحتيال فيمكن وقوعه على دون ذلك ،وغالبا ما تجتمع جريمتا التزوير و الاحتيال ، ونكون بذلك امام حالة التعدد المادي للجرائم ، كما يمكن ان تجتمع الجرمتين في فعل جرمي واحد [39] .

---

35 المحامي المتدرب عبد الرحيم السلايمة ، التزوير الالكتروني ، بحث مقدم لنقابة المحامبين الاردنيين لغايات استكمال متطلبات التسجيل في سجل المحامين الاساتذة ، عمان ، 2014 ، صفحة 7.

36 المحامي المتدرب عبد الرحيم السلايمة ، مرجع سابق ، صفحة 7 .

37 فتوح الشاذلي وعفيف كامل عفيف ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون ، دراسة مقارنة ، منشورات دار الحلبي الحقوقية ، بيروت ، 2003 ، صفحة 233 .

38 فتوح الشاذلي وعفيف كامل عفيف ، مرجع سابق ، صفحة 234 وما بعدها .

39 نعيم مغبغب ، حماية برامج الكمبيوتر – الاساليب و الثغرات ، دراسة مقارنة ، الطبعة الاولى ، منشورات دار الحلبي ، بيروت ، 2006 ، صفحة 217 .

ومما تجدر الاشارة اليه الى ان جريمة التزوير التقليدية تقوم على ركنين ،مادي و معنوي ، وهي لا تختلف عن جريمة التزوير الالكتروني في المجمل ، سوا انه يشترط حتى نكون امام جريمة تزوير الكتروني ان ترتكب الافعال المادية لجريمة التزوير من خلال كمبيوتر او حاسب آلي ،ولا يسعنا في هذا المقام التحدث عن هذا الموضوع هنا حيث سوف نخصص له مطلب مستقل في الفصل الثاني من الرسالة حتى نتعرف اكثر على اركان و عناصر جريمة التزوير الالكتروني .

واذا كان التزوير التقليدي (تحريف مفتعل) يقع على صك او مخطوط او مستند او ورقة وهو ما يطلق عليه بالمحرر ، فانه في النطاق الالكتروني هو (تعديل او تحريف او تحوير) ايضا ، يقع وفق الفقه الغالب على المستندات المعالجة الكترونيا (آليا) التي يمكن ان يحتج بها ، والمستندات المعالجة الكترونيا هي في حقيقتها البيانات والمعلومات والسجلات والملفات الالكترونية التي اتخذت صفة مستند يراد الاحتجاج به بوصفه مستندا ، لان المستند في نظام الكمبيوتر هو ملف ، ومحتوى الملف بيانات ومعلومات ، وللملف اشكال متعددة ، كالوثيقة المكتوبة او صورة الوثيقة المكتوبة او السجل ، فمحله من طبيعة معنوية لا طبيعة مادية ، تماما كالطبيعة المقررة للمعلومات [40].

ويفهم مما سبق بأن مفهوم التزوير لايثير صعوبة حيث ورد في كافة القوانين والتشريعات العقابية التقليدية ،ولكن التزوير بظهور تكنولوجيا وتقنية الحاسبات الآلية قد اكتسب بعد جديداً أضف عليه اهمية تفوق ما كان عليه قبل ذلككما اكسبته شكلاً جديداً بل تسميه جديدة حيث اصبح يشار اليه بالمعلوماتية اشارة يرتبط بها بتقنية تكنولوجيا الحاسبات .

وعلية فأن التزوير الالكتروني يرد على معلومات (بينات ومعطيات) محفوظة في وثائق معلوماتية وهي تلك الوثائق التي يتم الحصول عليها بوسائل معلوماتية، بعبارة ادق تلك الوثائق التي يتم الحصول عليها بواسطة جهاز اليكتروني او كهرومغناطيسي أو أشرطة ممغنطة وأن كان هنالك جانب من الفقه يرى ضرورة عدم الخلط بين الوثائق المبرمجة والوثائق المعلوماتية، وعلى الرغم مما ذكر فأن التزوير المعلوماتي يعادل في خطورته التزوير التقليدي وعليه فأن التزوير المعلوماتي هو أي تغيير للحقيقة في محرر بكل الطرق التي يقرها القانون المادية والمعنوية تغيراً من شانه احداث ضرراً للغير بواسطة استخدام الحاسب الألي[41] .

---

40 عمر الحسيني ، جرائم الكمبيوتر و الجرائم الاخرى في مجال تكنولوجيا المعلومات ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، 25-28 تشرين الاول ، 1993 ، صفحة 26 .

41 سامي الشوا ، الغش المعلوماتي كظاهرة اجرامية مستحدثة ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، 25-28 تشرين الاول ، 1993 ، صفحة 19 .

المطلب الثاني

محل جريمة التزوير الالكتروني

تمثل جرائم الكمبيوتر طائفة الجرائم المنصبة على المعلومات بمفهومها الواسع (بيانات،برامج تطبيقية،وبرامج تشغيل) ، اما بالنسبة للمكونات المادية للحاسوب ،فالموقف الغالب يتجه الى اعتبارها من قبيل الجرائم الواقعه في نطاق الجرائم التقلدية [42] .

من هنا ثارت التساؤلات لدى الفقه حول المعلومات و البينات التي يمكن ان تكون محلاً للأعتداءات وبالتالي تكون محل للحماية القانونية ، وقد انقسم الفقه حول ذلك الى رأيين :-

الراي الاول :-

يذهب الى أن المعلومات التي تصلح أن تكون جديرة بالحماية القانونية هي تلك المعلومات والبيانات ذات الطبيعة المادية بوصفها نشاط انساني، وضرورة ان يتحقق فيها عنصرين هما التجديد والأبتكار - من جهة- والسرية والأستئثار - من جهة اخرى ، **فالتجديد والابتكار** ميزة اساسية تفرض نفسها قبل كل شيء وبأنعدامها تزول حقيقة المعلومات، فالمعلومة قبل كل شيء تعبير وصياغة مخصصة من اجل تبليغ رسالة أو يمكن تبليغها عن طريق علامات او اشارات مختارة لكي تحمل الرسالة الى الغير، والمعلومة بوصفها رسالة مخصصة للتبليغ يجب أن تكون مادية بحيث تحسها عين الادمي، علاوة على المعلومة المادية المحددة يجب أن تكون مبتكرة، فالمعلومة وأن كانت مادية وان كانت محددة اذا كان الوصول اليها شائع ومن قبل الكافة فمن السهولة أن يقع الاعتداء عليها ، **أما بالنسبة للسرية** فهي صفة ملازمة للمعلومة من حيث انها ستحصر في نطاق محدد من الاشخاص وذلك لأن المعلومة غير السرية لها ميول للتداول والنقل لايمكن اعتبارها من قبيل المعلومات بمعناها الحقيقي، وكذلك الحال بالنسبة للأستئثار فأنه امر ضروري للمعلومة ايضاً ، لأنه في جميع الجرائم التي تنصب على البيانات المتداولة عبر شبكات الانترنت ليستأثر الجاني بسلطة تخص الغير وبصورة مطلقة . [43]

الراي الثاني :-

يذهب الى خلاف ذلك و يتمسك بأن المعلومات و البينات تصلح ان تكون محل للحماية القانونية حتى ولو لم تكن ذات طبيعة مادية ، ويبرر اصحاب هذا الاتجاة رأيهم بأن المعلومات و البينات

---

42 المحامي يونس عرب ، المدخل الى الجرائم المعلوماتية ، مرجع سابق ، صفحة 167 .
43 محمد عبدالله ابو بكر سلامة ، جرائم الكمبيوتر و الانترنت ، (موسوعة الجرائم المعلوماتية) دار النهضة العربية ، القاهرة ، 2004 ، صفحة 199.

تتميزبأنها ذات طبيعة معنوية من نوع خاص ، وبذلك تكون محلا للحماية التشريعية بسبب التقدم الهائل لصور و اشكال انظمة المعلومات و الاتصالات [44].

وان التباين في الاراء هذا انما مصدره عدم تحديد الطبيعة القانونية لمحل الاعتداء في جريمة التزوير الالكتروني ، حيث ان موضوع هذه الجريمة هو معطيات الحاسوب و التي يطلق عليها مسمى المعلومات الخام وهي التي تمثل المصلحة التي تهدرها هذه الجريمة و الحق الذي يعتدى عليه يتمثل بالحق في المعلومات ذاتها و التي قد تمثل اموال او اصول او اسرار او بينات شخصية ، الا ان ما يثيره تحديد الطبيعة القانونية للمعلومات من مشاكل أساسية في تحديد موضوع الجريمة من جهة ،وفي مسألة تطبيق نصوص القوانين الجنائية عليها من جهة اخرى ،تتصل بشكل رئيس بمسألة المسؤولية الجنائية عن هذه الافعال، فالمعلومات او كما يسميها البعض المال المعنوي اثارت و تثير مشكلة امكان انطباق النص القانوني الجزائي عليها كما هو شان انطباقة على الاموال المادية ،ومصدر المشكلة واساس الجدل الطبيعة المعنوية للمعلومات ونعني هنا المعطيات المجردة من وسائطها المادية ، اي ان اساس الجدل هو قابلية النص الجنائي الذي يحمي الاشياء المادية للانطباق على المعطيات ذات الطبيعة المعنوية ،ومن ثم تحدد القانون الواجب التطبيق من بين القوانين الجزائية المتصل بشكل مباشر بالمسوؤلية الجزائية عن الافعال المرتكبة [45] .

وعلية نخلص في هذا المقام الى حقيقتين:-

اولاهما : ان نصوص القوانين الجزائية قد حددت الفعل المجرم والجزاء المنطبق عليه تبعا لطبيعة محل الاعتداء، ومن خلال استعراض القوانين الجزائية نجدها قد كفلت من حيث الاصل ومن خلال نظرياتها و قواعدها حماية الاموال المادية و نصت بشكل مباشر في تجريم الاعتداءات الواقعه على الاموال بأنها الاعتداءات او التهديد الذي ينال من الحقوق ذات القيمة المالية ، كما نصت في تجريم اتلاف المال او الاصول (كجريمة ذات طابع مادي) وتجريم الاعتداء على الاعتبار في المحرارات الكتابية (وهي جرائم التزوير و التزيف) المنصبة على ماديات ، لذا فأن النصوص التقلدية في القانون الجزائي قد وضعت وفقا لمعيار" منقول مادي".

ثانيهما: طبيعة المعلومات محل جريمة التزوير الالكتروني، والتي تتسم بانها ذات طبيعة معنوية، قد اثارت جدلا واسعا كونها تخلو من السمة المادية ، والذي يطلق عليه الفقه "المال المعنوي"، واكثر ما يثار حوله من تساؤلات هو كيفية حماية المال المعنوي وكيفية تحديد

---

44 محمد عبدالله ابو بكر سلامة ، مرجع سابق، صفحة 200.
45 هدى حامد قاشوش ، الحماية الجنائية لمعطيات الكمبيوتر ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، 2000 ، صفحة 167.

نطاق الحماية الجزائية ، بمعنى اخر مدى انطباق النصوص الجزائية التي شرعت ابتداء لحماية مال مادي منقول لحماية مال معنوي [46] .

وان الحقيقتان المشار اليهما اعلاه، الطبيعة المادية للحقوق المالية التي يحميها القانون الجنائي، والطبيعة المعنوية لمعطيات الحاسوب، خلقتا اتجاهات متباينة في تحديد الطبيعة القانونية للمعلومات(معطيات الحاسوب) :-

فظهر اتجاه فقهي – الفقه الفرنسي تحديدا :- يعتبر المعلومات اموالا ذات طبيعة خاصة انطلاقا من ان غياب الكيان المادي للمعلومات لا يجعلها محلا لحق مالي من نوع الحقوق المتعارف عليها في الفقه والتي ترد على كيانات مادية، وان جاز اعتبارها محلا لحق ملكية ادبية او فنية او صناعية، وبالتالي فان المعلومات التي لا تكون متصلة بالنواحي الادبية والفنية والصناعية او التي تأبى بطبيعتها عن ان تكون محلا لمثل هذه الحقوق، يلزم بالضرورة استبعادها من طائفة الاموال، وليس من مقتضى هذا الاستبعاد ان تظل هذه المعلومات عارية عن اية حماية اذا ما جرى الاستيلاء عليها او استخدامها استخداما غير مشروع، فمثل هذا الفعل يعد (خطأ) يحرك مسؤولية فاعله والسائد لدى جانب من الفقه الفرنسي ان هذ المسؤولية تتحرك وفق قواعد المسؤولية المدنية المستندة الى نص المادة 1382 من القانون المدني الفرنسي، وبالاعتراف بالخطأ تكون المحكمة قد اعترفت بوجود الحق(وهو الحق في المعلومات)، مما مؤداه ان يكون للمعلومات طبيعة خاصة تسمح بان يكون الحق الوارد عليها من نوع الملكية العلمية .**اما الاتجاه الثاني** فهو الاتجاه الفقهي الاكثر ارتباطا بالمشكلات المتفرعة على الاستخدام الحديث للمعلومات ونظمها وبرامجها في اطار التقنية الحديثة، فقد اتجه هذا الفريق من الفقهاء الى بسط وصف " المال" على " المعلومات" في ذاتها مجردة عن دعاماتها المادية نظرا لقابليتها للحيازة و للتملك ،لكن كل الجدل دفع الى الوصول يوما بعد يوم الى حقيقة مفادها انه وفيما يتعلق بالمعلومات ونظمها وسبل معالجتها اليا، فان الامر لا ينبغي ان يترك للتفسير الفقهي والقضائي من اجل بسط النصوص القائمة عند الاعتداء على المعلومات، لذا فان الايسر والاصوب ان يلتفت المشرع الى هذه المشكلة بتشريع خاص ينص على تجريم صور العدوان على المعلومات ونظمها وبرامجها وسبل معالجتها لكون الاعتداء لم يعد مقصورا على الاستيلاء على المعلومات بقصد الغش فقط، بل انها تشمل الكثير مما ينبغي التصدي له بالتجريم وبالعقاب [47] .

---

46 يونس عرب ، جرائم الحاسوب ، دراسة مقارنة ، رسالة ماجستير مقدمة للجامعة الاردنية ، عمان ، 1994 ، صفحة 206- 211 .
47 يونس عرب ، جرائم الحاسوب ، دراسة مقارنة ، مرجع سابق، صفحة 206- 211 .
48 احمد حسام طه تمام ، الحماية الجنائية لتكنولوجيا المعلومات ، دار النهضة العربية ، القاهرة ، 2002 ، صفحة 299.

ونجد أن الهدف من تجريم الاعتداء على المعلومات بصورة عامة بغض النظر فيما اذا كانت ذات طبيعة مادية ام معنوية او اي امر اخر، هو تحقيق الثقة العامة بالمحررات بغض النظر عن طبيعتها ، وتوفير الحماية القانونية لكل ما تفرزه انظمة المعلومات من صور واشكال للجرائم المعلوماتية ومنها جريمة التزوير الالكتروني هذا من ناحية ، ومن ناحية اخرى فأنه سواء تم اخراج هذه المعلومات على مخرجات ورقية ام بقيت في ذاكرة الحاسب الآلي ووقع عليها اعتداء لطالما كات ذلك الاعتداء يسبب الضرر بالمصلحة العامة أو بمصلحة شخص من الاشخاص فأنه يعد تزويراً ، اما بالنسبة للقانون الواجب تطبيقه على تلك الأعتداءات فان الفيصل فيه هي الاداة المستخدمة بارتكاب فعل التزوير فأذا كانت الاداة المستخدمة الحاسوب عد تزويراً معلوماتي يخضع للتشريعات العقابية المعالجة لجرائم الانترنت، اما إذا وقع بأي طريقة من الطرق التي حددتها النصوص التقليدية وبدون استخدام الحاسب الألي فأنه يعد تزويراً تقليداً يخضع فاعله للعقاب المقرر في القوانين الوطنية [48] .

والحقيقة الثابته هي، ان معظم القوانين التي عالجت جرائم الانترنت والحاسب الألي- لاسيما القوانين والتشريعات العربية - لم تجر أي تعديل يتيح او يبين طبيعة المعلومات التي تصلح ان تكون محلا للحماية الجنائية حيث لم يشر الى ان هناك مساواة ما بين المعلومات ذات القيمة المادية والمعلومات ذات القيمة المعنوية، بعبارة اخرى بين الأشياء المادية الصالحة كمحل للاعتداءات وبين السلوكيات المعنوية كالمساواة مابين التزوير في الوثيقة الالكترونية والتزوير في المحرر العادي، بالإضافة الى أن قوانين الاتصالات العربية حينما شهدت ظهور وتطور في المجال الجنائي لم تتضمن نصوص تجرم الأعتداء على معلومات مادية واخرى معنوية وانما جاءت معظمها مطلقة وذلك لان المساس بالبيانات أو المعلومات بواسطة الحاسب الألي هو مساس جوهري .

وهنا نخلص الى نتيجة مفادها ان المعلومات (المعطيات والبيانات) هي محل جريمة التزوير الالكتروني، وهي مال ذو طبيعة معنوية، فلا بد من مراعاة خصائص الاموال المعنوية في سياسة الحماية الجنائية للمعلومات، ويتجلى الاختلاف في الحماية الجنائية للاموال المادية عن الحماية الجنائية للاموال المعنوية ، وذلك لما للاموال المادية من طبيعة تمكن صاحبها من الاستئثار بها بشكل محدد ومطلق بمعنى ان الحقوق الاستئثارية مقتصرة على الاموال المادية، اما المعلومات – وان صح التعبير – فهي مال شائع ، بمعنى انها وكشرط اساسي حرة، تستند الى مبدأ (حرية الوصول الى المعلومات)، مما يدفع الفقه الى القول بضرورة اتجاه التشريع الى زيادة الاسس الخاصة بحماية المعلومات، وذلك بشقين من السياسة التشريعية للحماية الجنائية للمعلومات ؛

الاول: يتعلق بحماية حرية انسياب المعلومات وتدفقها واستخدامها اعمالا لمبدأ (حرية الوصول الى المعلومات)، والثاني: الحماية الجنائية المنصبة على مواجهة الاعتداء على المعلومات [49].

49تركي نعيم شلال ، دعاوى التزوير الالكتروني ، دراسة مقارنه ، منشورات الحلبي الحقوقية ، لبنان ، 2000 ، صفحة 105.

المبحث الثاني

صور جريمة التزوير الالكتروني

ثمة عدة تقسيمات لصور التزوير التقليدي الواقع على المحررات ، اذ ثمة تقسيم يعتمد على نوع المحرر ووجوده ابتداء ، فنكون امام التزوير في مستندات رسمية ، والتزوير في اوراق خاصة ، والمصدقات الكاذبة (وهي المحررات المصطنعة التي ليس ثمة وجود مسبق لها) . وثمة تقسيم يتعلق بطبيعة طرق التزوير عموما ، فنكون امام التزوير المادي والمرتكب بعدة طرق ووسائل . والتزوير المعنوي المرتكب هو الاخر بعدة طرق ووسائل . وثمة تقسيم متصل بالطرق المتبعة لتغيير الحقيقة المرتكب بها التزوير ، وهذه غالبا ما يصعب حصرها لانها تتوقف على ما يقرره النص القانوني في التشريع العقابي بشان طرق تغيير الحقيقة [50].

اما التزوير الالكتروني ، فانه من حيث السلوك ايضا يكاد ينحصر في اربع عمليات لا اكثر ، اصطناع او خلق المستند او المعطيات ، الحذف او التدمير او الاتلاف ، الاضافة ، والاستبدال (تغيير بيان قائم) ، وهذه العمليات او الافعال - تبعا لموقف التشريع - اما ان ينص عليها بوصفها تستهدف المعطيات ايا كان شكلها ، او حصر محلها بالمستندات المعالجة آليا ، وجميعها تنطوي على تغيير الحقيقة سواء عبر اصطناع ملف او في ملف قائم ، وهذا بالتاكيد يثير التساؤل ما اذا كان يمكن ان يقع على مستندات رسمية ام مستندات خاصة [51] .

و نشير في هذا المقام الى ان التزوير الالكتروني التي ايدنا فيها موقف الفقه الغالب انما ينصب على الملفات المعالجة آليا (مستثنى منها البرامج الالكترونية) ، والتي قد يصح ان نطلق عليها اصطلاح المستندات المعالجة اليا او المستندات الالكترونية ، وهذه الملفات انما هي في اصلها ملفات خاصة لان الرسمية كما هو معلوم يقررها وسم المستند او المحرر بالخاتم الرسمي للدولة او ما يقوم مقامه من اختام المؤسسات والاجهزة الحكومية ، او يقررها طبيعة المستند او السجل المقر له ابتداء بصفة الرسمية من حيث الجهة التي تنظمه . واذا كان في بدايات تطبيقات تقنية المعلومات لم يكن متصورا ان يتم انشاء وتبادل المستندات الرسمية عبر شبكات المعلومات وانظمة المعلومات ، فاننا في ظل ما اصبح يعرف بالحكومة الالكترونية ، اصبحت السجلات الرسمية والمستندات الرسمية تنظم وتتبادل عبر المواقع الالكترونية ، وتخزن وتحفظ في انظمة المعلومات ، كما اصبح للمستخدمين مداخل على المعلومات الاكترونية الحكومية ، الى جانب انها في الاصل مخزنة ضمن

50كامل السعيد ، الجرائم الواقعة على الثقة العامة ، الطبعة الاولى ، منشورات دار الثقافة ، عمان ، 2001 ، صفحة .
51 عفيفي كامل عفيفي ، جرائم الكمبيوتر ، منشورات الحلبي الحقوقية ، الطبعة الاولى ، بيروت ، 2003 ، صفحة 177 .

نظم المعلومات الحكومية التي قد تتعرض الى انشطة الاختراق بقصد تزوير ما تتضمنه من بيانات او معلومات الكترونية [52] .

في هذا المبحث ، سنقف على صور التزوير الالكتروني من زاوية محل الجريمة (المطلب الاول) ، كما سنقف عليها من زاوية طرق تغيير الحقيقة- طريقة ارتكاب الفعل- في (المطلب الثاني) طبعا مع ما يقابل هذه الصور في التزوير التقليدي ان كان ثمة مقابل لها .

52عفيفي كامل عفيفي ، جرائم الكمبيوتر ، مرجع سابق ، صفحة 179 .

المطلب الاول

صور التزوير الالكتروني بالنظر الى محل الجريمة

تعرف التشريعات العقابية عموما ثلاث صور اساسية للتزوير في المحررات وذلك بالنظر الى محل الجريمة ، و هذه الصور هي التزوير في المستندات الرسمية ، والتزوير في الاوراق الخاصة ، وما يعرف بالمصدقات الكاذبة ، وتفترق الصورتان الاولى والثانية عن بعضها البعض بالنظر للمحرر محل الجريمة لا اكثر ، اذ يقع التزوير بذات الوسائل او الطرق المقررة في القانون . في حين تختلف الصورتان الاولى والثانية عن الصورة الثالثة بالنظر ايضا للمحرر ولكن من حيث وجوده ابتداءا وليس طبيعته ونوعه ، ففي المصدقة الكاذبة لا وجود اصلا للمحرر وانما اوجده مرتكب الفعل من العدم ، في حين في التزوير سواء في مستندات رسمية ام مستندات خاصة ثمة محرر موجود لحقه تغيير في الحقيقة بالمحو او الكشط او الاضافة او التحشية وباتباع واحدة من الطرق التي نص عليها القانون [53].

وبالرجوع الى قانون العقوبات الاردني ، نجده قد نص على اربع صور تحت عنوان التزوير :-

1- التزوير الجنائي ، وهو التزوير في مستندات رسمية يرتكبها الموظف العام او يرتكبها اي شخص غير موظف عام بالطرق المحددة المقررة في قانون العقوبات في المادتين 262 و 263 ، وقد نظمها المشرع الاردني في المواد 262 ولغاية 265 من قانون العقوبات . وهي جنايات تختص بنظرها محاكم البداية بصفتها الجنائية والتي تتكون هيئاتها من قاضيين .

2- المصدقات الكاذبة ، وهي في حقيقتها تزوير بصورة ايجاد مستند لا اصل له واستعماله كانه مستند اصلي صحيح ، سواء ارتكب الفعل موظف في حدود وظيفته باصدار شهادات غير صحيحة اصلا او ارتكبها شخص غير موظف، ويعد من قبيل المصدقات مذكرات التبليغ القضائية وشهادات حسن السلوك . وقد نظمها المشرع الاردني في المواد 266 ولغاية 268 من قانون العقوبات ، وحيث ان سقف العقوبة في جميع صورها لا يتجاوز سنة واحدة ، وهذا الحد باعتباره لا يتجاوز سنتين ، فان الاختصاص بنظرها يكون لمحكمة صلح الجزاء .

53كامل السعيد ، شرح قانون العقوبات الاردني ، الجرائم الواقعة على الاموال ، الطبعة الثانية ، دار الثقافة للنشر و التوزيع ، عمان ، 1991 ، صفحة 206 .

3- انتحال الهوية ، وهي صورة خاصة محصورة بتقدم احد الاشخاص الى سلطة عامة بهوية كاذبة بقصد جلب منفعة لنفسه او غيره او بقصد الاضرار بالغير ، وقد نظمها المشرع في المادتين 269 و 270 من قانون العقوبات ، وهي من اختصاص محكمة صلح الجزاء لان سقف العقوبة فيها الحبس لمدة سنة .

4- التزوير في الاوراق الخاصة ، وهي جرائم التزوير التي ترتكب بذات الطرق التي ترتكب بها جنايات التزوير في الاوراق الرسمية المنصوص عليها في المادتين 262 و 263 من قانون العقوبات ، وقد نظم المشرع التزوير في الاوراق الخاصة في المادتين 271 و 272 من ذات القانون ، وحدد سقف العقوبة فيها الحبس لثلاث سنوات وهو ما يجعلها جنحا بدائية وتختص بنظرها محكمة بداية الجزاء بصفتها الجنحية وينظر الدعوى قاض واحد .

وباستثناء الصورة الثالثة المتمثلة بانتحال الهوية ، والمنظمة في المادتين 269 و 270 من قانون العقوبات، فان الصور الثلاث الاخرى – كما في مختلف قوانين العقوبات المقارنة - تتعلق بالتزوير في المحررات . ويتسم المحرر بثلاث سمات رئيسة :-

1- ان يتخذ شكلا كتابيا ، والشكل الكتابي يتضمن الحروف والرموز بغض النظر عن لغته ، كما لا يهم نوع الوعاء الورقي المفرغ فيه المحرر ولا اداة كتابته ان كانت يدوية ام آلية ، كما لا يهم ان كان عقدا او سندا او سجلا ، وقد يكون بسيطا (كسند الدين) او مركبا (كمحاضر الشهود) ، لكن اهم عنصر في هذه السمة ، هي ادراك المحرر او السند بالبصر ، وهو العنصر الذي وجد كسبب رئيس في عدم امكان تطبيق نصوص تجريم التزوير التقليدي على معطيات الكمبيوتر وحاجة انشطة التحريف التي تقع عليها الى نصوص تجريم خاصة ، وسوف نعود لهذه المسالة لدى بحث موقف قانون المعاملات الالكترونية الاردني المؤقت رقم 85 لسنة 2001.

2- ان تكون الكتابة منسوبة لشخص معين ، اذ يتعين نسبة الكتابة او امكان نسبتها الى شخص بعينه .

3- ان يحدث المحرر اثرا قانونيا ، لان الحماية انما لا تنصب على متن المحرر وانما على المصالح والحقوق التي يثبتها المحرر وبالتالي لا بد ان يكون له اثر في هذا الشان [54].

وبالعودة الى التزوير الالكتروني ، فان محله من حيث الاصل المعطيات او البيانات والمعلومات الالكترونية ايا كان شكلها ، واختيار شكل المحل يحدد نطاق جريمة التزوير الالكتروني ويميزها عما قد يختلط بها من جرائم الكترونية اخرى ، وتحديدا جريمة العبث بالمعطيات كاثر للدخول غير المصرح به الى نظام المعلومات .

ومن حيث محل جريمة التزوير الالكتروني ، وباعتبار التزوير تغيير في الحقيقة ، فان الاصل ان تكون معطيات الكمبيوتر باي صورة تتخذها محلا لهذه الجريمة في مقابل المحرر الذي هو محلها في التزوير التقليدي ، لكن هذا القول يضعنا امام عدة صور تبعا لاختلاف المحل ، جزء منها لا يدخل في نطاق مفهوم التزوير الالكتروني في بعض التشريعات كالقانون الفرنسي مثلا ، لكنها تدخل مثلا في مفهوم النص الدولي الذي اوردته اتفاقية بودابست الخاصة بالجرائم الالكترونية لعام 2001 ، مكتفين بالقول هنا ان اتفاقية بودابست للجرائم الالكترونية 2001 جعلت معطيات الكمبيوتر Computer Data محلا للتزوير ، ومعلوم ان معطيات الكمبيوتر تعبير واسع يشمل جميع اشكال الملفات والسجلات واية اشكال تتضمن بيانات او معلومات مدخلة ومخزنة ومعالجة في نظم الكمبيوتر او ما اصبح يطلق عليها انظمة المعلومات [55].

فوفق المعنى الضيق للتزوير الالكتروني ، وباعتبار الكمبيوتر مجرد اداة لارتكابه لا اكثر ، يكون للتزوير صورة واحدة وهو التزوير المنصب على المستندات المعالجة آليا ، وهو ما يفترض اننا امام مستندات موجودة في الاصل بصورة تقليدية او كانت تتخذ شكلا ورقيا في السابق ادخلت الى الكمبيوتر كنماذج الكترونية في اطار معالجتها آليا او رقميا ، وهي التي تكون محلا لجرم التزوير الذي يستهدف التغيير في مشتملاتها بالحذف والاضافة والتعديل . وهذا هو موقف المشرع الفرنسي الذي جرم التزوير الالكتروني تحت هذا الوصف ، في حين جرم اي تغيير او تعديل او

---

54 هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الالات الكاتبة ، اسيوط **1995** ، صفحة **323**.

55 المحامي يونس عرب ، ورقة عمل ((قانون جرائم انظمة المعلومات) ورشة عمل لمناقشة التشريعات السيبرانية ، نقابة المحامين الاردنيين ، **2010/8/23** .

حذف او اتلاف لمعطيات الكمبيوتر ضمن صور الدخول غير المصرح به ولتمييزهما عن بعضهما، اشترط لقيام التزوير وقوعه على مستند معالج آليا او الكترونيا ، واشترط حصول ضرر بالغير [56].

لكن ثمة معنى واسع للتزوير الالكتروني ، نجده في ادوات تشريعية عديدة ، منها المعنى المستفاد من المادة 7 من اتفاقية بودابست للجرائم الالكترونية لسنة 2001 ، والمعنى المستفاد ايضا من نظام مكافحة الجرائم المعلوماتية السعودي لسنة 2007 مع مراعاة الاختلاف بينهما ، فبالنسبة لاتفاقية بودابست ، يجري نص المادة 7 منها الباحثة بالتزوير المتعلق بالكمبيوتر (كما اسمته) على النحو التالي :- ((تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير اخرى لتجريم الافعال التالية في قانونها الوطني ، اذا ما ارتكبت عمدا ، وبغير حق :- ادخال ، او تبديل او محو ، او تدمير معطيات كمبيوتر ، ينتج عنها معطيات غير اصلية بقصد استخدامها او التعويل عليها في اغراض قانونية كما لو كانت اصلية ، بغض النظر عما اذا كانت هذه المعطيات مقروءة ومفهومة بشكل مباشر من عدمه ، ويجوز لطرف ان يشترط وجود نية الغش (التدليس) او وجود قصد غير امين مشابه (سوء النية) لقيام المسؤولية الجزائية)) ، فمحل الجريمة وفق النص المتقدم هو معطيات الكمبيوتر . ولكي يكون الفعل الواقع عليها تزويرا استلزم النص تحقق نتيجة وهي انتاج معطيات غير اصلية مقروءة ام غير مقروءة بشريا ، اي مدركة او غير مدركة بالبصر . ويشترط ان يعول عليها لاغراض قانونية ، اي تصلح لاكتساب حقوق وحماية مصالح ، وان يتم الفعل بقصد خاص هو الاستخدام او الاستعمال ، مع امكان كل مشرع وطني ان يضيف اي قصد خاص آخر ، واما النص السعودي كمثال آخر ، وهو نص المادة 1/5 من نظام مكافحة الجرائم المعلوماتية لسنة 2007 ، والسابق عرضه فيما تقدم ، نجده يتضمن تجريم (الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها)) فالمحل هو البيانات (الخاصة) ، وقد عرف البيانات بانها ((المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، كالأرقام والحروف والرموز وغيرها)) . في وقت تضمن نفس النظام تعريفا لبرامج الكمبيوتر لاخراجها من دائرة (البيانات) [57].

وبتحليل هذين النصين (نص اتفاقية بودابست والنص السعودي) ، واجراء المقارنة ما بينهما ، وما بينهما وبين النص الفرنسي السابق بيانه ، نجد ان المحل في النصين متسع ، ويشمل من حيث الاصل المستندات المعالجة آليا ، وجميع الملفات الالكترونية باي صورة كانت عليه هذه

---

56 المحامي يونس عرب ، قانون انظمة المعلومات الاردني ، ورقة عمل مقدمة ضمن ورشة عمل التشريعات الالكترونية – الاسكوا الامم المتحدة ونقابة المحامين الاردنيين واتحاد المحامين العرب ، عمان ، 8-9 كانون الاول 2013

57 المحامي يونس عرب ، تطور التشريعات السيبرانية في الدول العربية ، ورقة عمل مقدمة الى ورشة الخبراء الاقليمية حول التشريعات السيبرانية لدى الاسكوا – الامم المتحدة ، 13-14 تشرين ثاني ، بيروت ، صفحة 29.

الملفات ، واية بيانات او معلومات مخزنة في النظام ايا كان شكل عرضها ، وثيقة او سجلا او غيره ، وايا كان النوع التقني للملف الذي تتضمنه ، ونجدها اكثر من ذلك تمتد لبرامج الكمبيوتر في نص اتفاقية بودابست لانها تتحدث عن معطيات الكمبيوتر ، في حين هي لا تشمل البرامج في النظام السعودي لان تعريف البيانات يخرجها من نطاقه ولان للبرامج تعريف خاص في النظام (القانون) ، مع ملاحظة ان اتفاقية بودابست قررت اركانا وعناصر تتيح وصف الفعل بانه تزوير الكتروني لتمييزه عن صور العبث الاخرى بالمعطيات التي تستهدف سرية وسلامة وتوفر المعطيات المنصوص عليها في ذات الاتفاقية ، في حين جرم المشرع السعودي العبث بالبيانات دون ان يجرم سلوكا يمكن وصفه بانه تزوير الكتروني ولم يقرر للعبث غير المشروع بالبيانات اية اركان او عناصر مما هو مقرر للتزوير كقصد الاستعمال او الحاق الضرر او غيرهما [58].

وعلية ان التزوير الالكتروني من حيث المحل يتخذ عدة صور تبعا للنص القانوني ، فقد يمتد الى كل معطيات الكمبيوتر او المعلومات الالكترونية فيقع من حيث المحل على كل ملف او سجل او مستند داخل النظام . وقد يكون محصورا من حيث محله بالمستندات المعالجة آليا ، او لنقل محررات اتخذت الطبيعة والشكل الالكتروني ، لكن في الحالتين ذهبت جميع التشريعات الوطنية الى عدم وقوع التزوير (بهذا المسمى) على البرامج كما اسلفنا بالرغم من انها معطيات من حيث طبيعتها وبناؤها ، ذلك لان التغيير او الحذف او الاضافة او الاقتباس او التقليد مجرم بموجب تشريعات حق المؤلف او تشريعات الملكية الفكرية (الادبية والفنية) التي اعتبرت البرامج مضنفات محمية بموجب نظام الملكية الفكرية وما يقع عليها من اعتداءات يوصف بانه افعال قرصنة او تقليد او تعدي على حق المؤلف لا تزويرا [59].

بقي في هذا المقام ان نجيب على التساؤل السابق طرحه ، هل يمكن تصنيف التزوير الالكتروني بتزوير الكتروني في مستندات الكترونية رسمية وآخر في مستندات خاصة :-

ان غالبية التشريعات تتضمن نصا يشدد العقوبة على سائر الافعال الجريمة التي تضمنها التشريع ان كانت المعطيات او البيانات حكومية ، وهي عقوبات اعلى من تلك المقررة للبيانات او المعطيات الخاصة . وبالتالي ان كان محل التزوير حسب النص هو المعطيات او البيانات او المعلومات الالكترونية فان ثمة تزوير في بيانات او معطيات رسمية وآخر في بيانات خاصة يفترقان من حيث العقوبة. اما ان كنا امام تشريع يقرر محل التزوير ويحصره في المستندات المعالجة اليا ، فاننا نكون امام تزوير في مستند رسمي معالج الكترونيا وتزوير في مستند خاص

---

58 المحامي يونس عرب ، تطور التشريعات السيبرانية في الدول العربية ، مرجع سابق ، صفحة 30 .

59 المحامي يونس عرب ، تطور التشريعات السيبرانية في الدول العربية ، مرجع سابق ، صفحة 32 .

معالج الكترونيا تبعا لنوع المستند ، سيما ان ثمة كثير من المستندات الرسمية او الحكومية الموضوعة بين يد الجمهور بصورة آلية مع اتساع نطاق توظيف التكنولوجيا في الخدمات الحكومية وفي ظل ما اصبح يعرف بالحكومة الالكترونية ، مع التنبه ان هذا الامر يجب ان يتضمنه التشريع الخاص بالجريمة الالكترونية بصورة واضحة ، لانه لا يمكن تطبيق قواعد ومفاهيم واحكام التشريع العقابي العام عن طريق القياس لان القياس محظور في النصوص الجزائية الموضوعية [60].

60 اسامة عبدالله قايد ، الحماية الجنائية للمحرارات في جرائم الكمبيوتر ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، 1996 ، صفحة 208 .

المطلب الثاني

صور التزوير الالكتروني بالنظر الى طريقة ارتكاب الفعل

التزوير التقليدي لا يقع الا بالطرق التي نص عليها القانون ، ففي القانون الاردني مثلا ، وكما اوردنا اعلاه لا يقع التزوير ، سواء في المستندات الرسمية او المستندات الخاصة الا بالطرق التي نصت عليهما المادتان 262 و 263 من قانون العقوبات ، وهذه الطرق هي :-

1- اساءة استعمال إمضاء او ختم او بصمة أصبع او إجمالاً بتوقيعه امضاء مزوراً .
2- حذف او إضافة تغيير في مضمون صك او مخطوط.
3- إتلاف السند إتلافا كلياً او جزئياً.
4- اساءته استعمال إمضاء على بياض اؤتمن عليه الشخص .
5- تدوين الموظف عقوداً او أقوالاً غير التي صدرت عن المتعاقدين او التي أملوها.
6- اثبات الموظف وقائع كاذبة على انها صحيحة او وقائع غير معترف بها على انها معترف بها او بتحريفه أية واقعة أخرى بأغفاله أمراً او إيراده على وجه غير صحيح.
7- ادخال الموظف قيدا في السجل يتعلق بمسألة جوهرية مع علمه بعدم صحة ذلك القيد [61].

اما التزوير الالكتروني ، فان وصف عمليات مفردات الفعل الذي يستهدف تغيير الحقيقة في المعطيات الالكترونية او في المستند المعالج آليا ام غير متصور ، فالفكرة في السلوك هنا احداث تغيير في الملف بصورته الاصلية ، لذا توصف عمليات التزوير الالكتروني بالسلوك العام لا بتفاصيله ، ولهذا فان صور التزوير الالكتروني الواقعة في نطاق تغيير الحقيقة تتمثل بما يلي :-

1- **اصطناع او خلق المستند او المعطيات :-** اننا في هذه الصورة لا نكون امام مستند معالج اليا او الكترونيا موجود في نظام المعلومات (الكمبيوتر) او مخزن باية وسيلة او واسطة تخزين الكرتونية ، بل نكون امام سلوك يقوم على ايجاد هذا الملف بما يحتويه من بيانات او معلومات وبالشكل الذي يتخذه ، سجلا كان ام مستندا ، ويكون الغرض من ايجاده او خلقه استعماله في امر ذو اثر قانوني .
2- الحذف او التدمير او الاتلاف كليا او جزئيا .
3- الاضافة .
4- الاستبدال .

---

61 المحامي يونس عرب ، ورقة عمل ((قانون جرائم انظمة المعلومات) مرجع سابق .

وهذه الصور الثلاث (الحذف او التدمير ، الاضافة ، الاستبدال) تلتقي من حيث وقوع السلوك فيها على ملف موجود داخل النظام او متبادل بين الانظمة عبر شبكات المعلومات وتطبيقات خزن الرسائل والوثائق والمعطيات ، والفعل هنا يستلزم ابتداء دخول الشخص الى نظام المعلومات (الكمبيوتر) ، والدخول هنا قد يكون دخولا مشروعا مصرحا به ، كدخول موظف البنك على قاعدة بيانات حسابات الزبائن المصرح له دخولها ضمن مهام وظيفته العادية ، او يكون دخولا غير مصرح به ، وهو يكتسب هذا الوصف سواء كان دخولا لشخص لا صلة له ابتداء بنظام المعلومات المعني ، او دخولا من قبل شخص مخول بالدخول اصلا لكنه ليس مصرحا له الوصول الى الملف او البيانات التي مارس عليها افعال التغيير بالحذف او الاضافة او الاستبدال [62] .

وانشطة اختراق الانظمة ، والمعروفة بقرصنة الهاكرز ، تكون لاهداف متعددة ، بعضها لمجرد اثبات القدرة على اختراق النظام ، في حين بعضها لاحداث تغيير في البيانات ، او اتلافها ، او الاستفادة منها بالاطلاع ، او نسخها والاستيلاء عليها . ومنها اختراقات تستهدف الوصول الى مستندات معالجة الكرتونيا داخل النظام بقصد تغيير ما تضمنته واستعمالها لتحقيق منافع او الحاق ضرر بالغير . وهذه الحقيقة بشان عمليات الاختراق هي التي استوجبت التمييز بين افعال العبث في البيانات كاثر للدخول غير المشروع للنظام ، وبين افعال التزوير الالكتروني التي تستهدف استعمال المعطيات التي جرى العبث بها لاحداث اثر قانوني [63].

وهذه الافعال اما ان تكون حذفا ، او اضافة ، او استبدالا (تغيير) . ومن غير المتصور ان تكون اكثر من ذلك ، ولهذا اهميته في استخدام الاصطلاحات القانونية الدالة على العمليات التقنية، اذ نجد بعض التشريعات – وابرز امثلتها قانوننا الاردني- قد لحقها خلل في استخدام الاصطلاحات ظنا من المشرع انها اصطلاحات مختلفة وهي في حقيقتها مترادفة ، فمثلا استخدم للحذف التدمير او الالغاء او المحو وجميعها تعبر عن ذات الفعل ، واستخدم للاستبدال التعديل والتغيير وغيرها [64].

ومن الناحية التقنية ، وكما سبق وذكرنا ، فكل دخول على ملف موجود واحداث اي عملية فيه ، كالحذف والاضافة والاستبدال ، هو تغيير . والى جانب التغيير ثمة عمليتان تقنيتان فقط تقع على الملفات ، خلق الملف او اصطناعه ابتداء ، والاتلاف الكلي للملف بحيث لا يبقى موجودا في النظام . واما كل ما يحدث من عمليات مشروعة على الملف بعد خلقه كنقله او تبادله انما هي عمليات معالجة [65] .

62 سعيد عبد اللطيف حسن ، جرائم الكمبيوتر ((جريمة التزوير المعلوماتي)) دراسة مقارنه ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، 1999، صفحة 210 وما بعدها .

63 هدى قشقوش ، الاتلاف العمدي لبرامج و بينات الحاسب الالكتروني ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ،25-28 تشرين الثاني1993 ، صفحة 22 .

64 سعيد عبد اللطيف حسن ، مرجع سابق ، صفحة 211 وما بعدها .

65 هدى قشقوش ، الاتلاف العمدي لبرامج و بينات الحاسب الالكتروني ، مرجع سابق ، صفحة 24 .

الفصل الثاني

اركان جريمة التزوير الالكتروني وموقف القانون الاردني منها

تمهيد و تقسيم :-

تقوم جريمة التزوير على ركنين ، مادي و معنوي ، وان كان جانب من الفقة يجعل من بعض عناصر الركن المادي ، كالضرر ، ركنا مستقلا بذاته وهذا العنصر ثار بشأنة الخلاف حول موقعه ، الا ان السائد في الفقة اعتباره عنصرا من عناصر الركن المادي ، اما الركن المادي فيقوم على تغيير الحقيقة بأي طريقة يقرها القانون وان يترتب على تغير الحقيقة ضرر ،وان ينصب هذا التغير للحقيقة على سند او وثيقة او محرر، وان يتم تغير الحقيقة باستخدام جهاز اليكتروني (الحاسب الآلي)[66].

وتغير الحقيقة وحده ، غير كاف في القانون ، وانما يلزم ان يتم باحدى الطرق المحددة حصرا في القانون ، و التي تقسم عموما الى طرق مادية تنال مادة المحرر و شكلة ، وطرق معنوية ، تنال مضمون المحرر او ظروفة او ملابساته دون المساس بمادته او شكله ، ويكتمل الركن المادي بتحقق الضرر الناتج عن تغير الحقيقة ، وان يتم فعل التزوير المتمثل بتغير الحقيقة من خلال (الحاسب الآلي)[67] .

اما الركن المعنوي لجريمة التزوير ، فيتخذ صورة القصد الجنائي ، ولا يكفي فيه القصد العام الذي يقوم على علم المتهم باركان الجريمة ، واتجاه ارادته الى الفعل المكون لها و تحقيق نتيجته ، بل تتطلب هذه الجريمة توافر قصد جنائي خاص ، يتمثل بنية استعمال المحرر المزور فيما وزر من اجله وعلى هذا فان القصد الجنائي في جريمة التزوير يعرف على نحو غالب لدى الفقه و القضاء بانه " تعمد تغير الحقيقية في محرر تغيرا من شانه ان سيبب ضررا و بنية استعمال المحرر فيما غيرت من اجلة الحقيقية [68] .

66فتوح الشاذلي وعفيف كامل عفيف ، مرجع سابق ، صفحة 250.
67فتوح الشاذلي وعفيف كامل عفيف ، مرجع سابق ، صفحة 250 .
68فتوح الشاذلي وعفيف كامل عفيف ، مرجع سابق ، صفحة 251.

وقد نص قانون العقوبات الاردني على جرائم التزوير في الفصل الثاني من الباب الخامس تحت عنوان الجرائم المخلة بالثقة العامة (المواد 260 – 272) ، وساوى في العقوبة في المادة 261 بين مرتكب التزوير ومستعمل المحرر المزور .

وسوف نقسم هذا الفصل الى مبحثين ، نتناول في المبحث الاول الركن المادي و الركن المعنوي لجريمة التزوير الالكتروني ، و نقسم هذا المبحث الى مطلبين الاول عناصر الركن المادي لجريمة التزوير الالكتروني ، الثاني عناصر الركن المعنوي لجريمة التزوير الالكتروني ، ثم نتناول في المبحث الثاني موقف القانون الاردني من جريمة التزوير الالكتروني بوصفها من جرائم انظمة المعلومات ، ونقسم هذا المبحث الى مطلبن **(المطلب الاول) نخصصة** لقانون المعاملات الالكترونية **،و (المطلب الثاني)** نخصصة لقانون جرائم انظمة المعلومات **.**

المبحث الاول

الركن المادي و الركن المعنوي لجريمة التزوير الالكتروني

تقوم جريمة التزوير على ركنين ، مادي و معنوي ، اما الركن المادي فيقوم على تغيير الحقيقة بأي طريقة يقرها القانون وان يترتب على ذلك ضرر ،وان يقع الفعل على سند او وثيقة او محرر ،وان يرتكب الفعل باستخدام جهاز اليكتروني (الحاسب الآلي) .

و الركن المعنوي لجريمة التزوير ، فيتخذ صورة القصد الجنائي ، ولا يكفي فيه القصد العام الذي يقوم على العلم والارادة ، بل تتطلب هذه الجريمة توافر قصد جنائي خاص ، يتمثل بنية استعمال المحرر المزور فيما اعد له .

المطلب الاول

عناصر الركن المادي لجريمة التزوير الالكتروني

الركن المادي :- لتحقق الركن المادي في جريمة التزوير الالكتروني لابد من تغيير الحقيقة في سند او محرر او وثيقة بأي طريقة يقرها القانون وبأستخدام الحاسب الألي ومن هذا يتضح ان الركن المادي في الجريمة محل الرسالة يتكون من ثلاثة عناصر :-

1- تغيير الحقيقة بأي طريقة يقرها القانون ،وان يترتب على تغير الحقيقة ضرر .

2- سند او وثيقة او محرر.

3- استخدام جهاز اليكتروني (الحاسب الآلي) [69].

وتغيير الحقيقة هو العنصر الاول من عناصر الركن المادي لجريمة التزوير الالكتروني وهو يمثل السلوك الاجرامي الذي يقوم به التزوير فاذا انتفى انتفت الجريمة . ولا يشترط ان يكون التغير كليا ، أي ابدال كل البيانات بما يخالف الحقيقة ، ويكفي ان يكون تغيير الحقيقة جزئيا او نسبيا ، والمستقر في الفقه ان المقصود في التزوير ، ليس تغيير الحقيقة الواقعية المطلقة ، وانما تغيير الحقيقة النسبية [70].

كما ان تغيير الحقيقة وحده في جريمة التزوير التقليدية غير كاف وفق نصوص القانون الناظمة لهذه الجريمة ، وانما يلزم وفق غالبية ان لم يكن جميع التشريعات العقابية الوطنية ان يتم باحدى الطرق المحددة حصرا في القانون ، والتي تقسم عموما الى طرق مادية تنال مادة المحرر وشكله ، وطرق معنوية ، تنال مضمون المحرر او ظروفه او ملابساته دون المساس بمادته او شكله ، وقد نصت المادتان 262 و 263 من قانون العقوبات الاردني على هذه الطرق في نطاق تزوير المستندات الرسمية ، كما قررت المادة 271 قيام التزوير في المستندات الخاصة بذات الطرق ، وهذه الطرق الي نصت عليها المادة 262 هي (اساءة استعمال إمضاء او ختم او بصمة أصبع او إجمالاً بتوقيع امضاء مزورا ، وبصنع صك او مخطوط وبما يرتكبه من حذف او إضافة تغيير في مضمون صك او مخطوط) وهذه كما هو واضح الطرق المادية للتزوير او تغيير

---

69 منير محمد الجنبيهى ، جرائم الانترنت و الحاسب الالي و وسائل مكافحتها ، دار الفكر الجامعي ، الاسكندرية ، 2004 ، صفحة 218.

70 محمد السعيد رشدى ، الجوانب القانونية لنظم المعلومات ، دار النهضة العربية ، القاهرة ، 2004 ، صفحة 120 .

الحقيقة ، واما الطرق التي نصت عليها المادة 263 والمتعلقة بالسند الذي ينظمه الموظف او السجل الذي في عهدته فهي على التوالي ((اساءته استعمال إمضاء على بياض اؤتمن عليه. او بتدوينه عقوداً او أقوالاً غير التي صدرت عن المتعاقدين او التي أملوها ، او باثباته وقائع كاذبة على انها صحيحة او وقائع غير معترف بها على انها معترف بها او بتحريفه أية واقعة أخرى بأغفاله أمراً او إيراده على وجه غير صحيح.)) وكذلك (أدخال قيد في سجل يتعلق بمسألة جوهرية مع علمه بعدم صحة ذلك القيد) . ويلاحظ ان النص هنا يتحدث عن الطرق المعنوية للتزوير او تغيير الحقيقة [71].

كما ويتم تغيير الحقيقة بنشاط ايجابي فأنه يمكن ان يتحقق بنشاط سلبي (الترك) ، وذلك إذا ترتب علىالترك تغييراً جوهرياً سبب ضررا للغير لأن الترك يعتبر تغيير للحقيقة وبالتالي يعد تزويراً معلوماتي او الكترونيلاسيما إذا كان الترك متعمداً وليس على سبيل الخطأ أو السهو[72].

وبالمقابل ، فان تغيير الحقيقة في نطاق جريمة التزوير الالكتروني لا يختلف عن معناه المقرر في التزوير التقليدي من حيث الاصل ، والامر رهن بما ذا كان النص القانوني قد حدد وسائل وطرق محددة يقع فيها التزوير الالكتروني . **اما عن تغيير الحقيقة من حيث هو شطب او اضافة او محو او تعديل او تحشية او نحوه ، فهو حاصل في كلا النوعين من التزوير** . وفي التزوير الالكتروني ينصب السلوك على مستند معالج الكترونيا وهو على ثلاثة انواع ، اما ملف رقمي محتو على بيانات يشكل لدى استخراجه ورقيا صورة مستند معالج الكترونيا (كوثيقة من نوع word مثلا)، او هو صورة مستند ورقي ادخل كصورة على جهاز الكمبيوتر فاصبح ملفا (كملفات PDF) ، او هو سجل الكتروني من سجلات النظام امكن الدخول اليه وتعديل قيد في قيوده بالاضافة او المحو او التعديل [73] .

ونجد هنا أن تغير الحقيقة في جريمة التزوير الالكتروني يكون من خلال ابدالها بغيرها ، ويتم اما بواسطة أدخال البينات او محوها او تحويرها ، و تغيير الحقيقة في التزوير الالكتروني يتم بأي طريقة يقرها القانون المعالج لهذه الجريمة **كأدخال** بعض البيانات أو المعلومات الى برنامج من خلال استغلال الاخطاء والعيوب المنطقية التي يحويها هذا البرنامج والتي لايمكن اكتشافها إلا عند

---

71 كامل السعيد ، شرح قانون العقوبات الاردني ، الجرائم الواقعة على الاموال ، مرجع سابق، صفحة 245 .
72 فوزية عبد الستار ، شرح قانون العقوبات ، القسم الخاص ، مرجع سابق ، صفحة 218 وما بعدها .
73 كامل السعيد ، جرائم الكمبيوتر و الجرائم الاخرى في مجال التكنولوجيا ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ،25-28 تشرين اول 1993 ، صفحة 44 .

استخدامه عن طريق المداخلة المميزة لتلك البرامج والتي هي في حقيقتها عبارة عن ممرات خالية ومتروكة في البرناج ويمكن استغلال هذه المحررات المعيبة فنياً بإضافة أي معلومات أليها[74] .

اما تغيير الحقيقة بواسطة محو بعض أو كل البيانات فهو يتم من خلال الحذف او الشطب ، كم هو الحال بالنسبة للشخص الذي دخل على برنامج سجلات الشرطة وقام بحذف بعض أسماء المجرمين المطلوبين للعدالة ،ويتحقق تغير الحقيقة ايضاً بأتلاف كل أو بعض البيانات ولكن لايعد تزويراً إذ وقع الاتلاف على البرنامج الذي تحويه تلك البيانات او المعلومات لأننا هنا لا نكون بصدد جريمة التزوير المعلوماتي وانما نكون اما جريمة اخرى (جريمة اتلاف المعلومات) [75] .

وإخيراً يتم تغيير الحقيقة بتحوير المعطيات والبيانات التي تمت معالجتها بأتباع اجراءات اليكترونية معينة ويتم هذا التحوير في المعطيات من خلال استخدام الحاسبات الالية لطبع فواتير مصطنعة او فواتير ذات قيمة كبيرة ويقوم العملاء بتسديدها منخدعين في الثقة التامة التي يتوسمونها في تلك الحاسبات. ومثال ذلك أيضاً العاملين في شركة تأمين بولاية لوس أنجلوس الامريكية والتي اختلقت بفعل حاسبها الألي وبمعاونة مبرمجيها عدداً وهمياً من المؤمن عليهم بملغ حوالي 64 الف وبثقة تأمين وقد تقاضت تلك الشركة من اتحاد الشركات التأمين في الولايات المتحدة عمولة نظيرا اجمالي لتلك الوثائق في حين اقتصر دورها فقط على ادارة الحسابات، وامعاناً في الغش ولغرض اعطاء العقود الوهمية مظهراً مشابهاً للحقيقة فقد قامت الشركة المذكورة بتفعيل الملفات المختلفة عن طريق تغيير الوطن والوظيفة وبعض البيانات الاخرى [76].

وعليه فأن تغير الحقيقة كعنصر من عناصر الركن المادي لجريمة التزوير الالكتروني تقع على البيانات والمعلومات بأي لغة كانت وبأي طريقة وجدت حيث لايهم المادة التي كانت عليها ولايهم شكلها سواء كانت صوراً ام رموز ام علامات ويستوي ان يكون التغير مادياً ومعنوياً اذا لم يشترط في تغيير الحقيقة التقليدية ان تكون بطريقة معينة .

ولا بد من الاشارة هنا الى انه حتى يكتمل العنصر الاول من عناصر الركن المادي في جريمتي التزوير التقليدية والالكترونية يجب ان يترتب على تغير الحقيقة **ضرر** ناتج عن تغيير الحقيقة ، والضرر كما يعرفه الفقيه محمود نجيب حسني ، " اهدار حق واخلال بمصلحة مشروعة يعترف بها القانون ويكفل لها حمايته" ،وبانتفاء الضرر ينتفي التزوير حين يتطلب النص ذلك ،

74منير محمد الجنبيهى ، جرائم الانترنت و الحاسب الالي و وسائل مكافحتها ، مرجع سابق ، صفحة 222.
75منير محمد الجنبيهى ، جرائم الانترنت و الحاسب الالي و وسائل مكافحتها ، مرجع سابق ، صفحة 222.
76اسامة عبدالله قايد ، الحماية الجنائية للخصوصية و بنوك المعلومات ، دار النهضة العربية ، طبعة 2 ، القاهرة 1999 ، صفحة 277 .

وللضرر انواع متعددة ، قد يكون ماديا او معنويا او ضررا احتماليا او ضررا اجتماعيا. وتشير مختلف المراجع المتصلة بجرائم الكمبيوتر او الجرائم الالكترونية الى اتفاق الفقه على وجوب توافر عنصر الضرر ليتحقق قيام الركن المادي لجريمة التزوير الالكتروني [77].

اما العنصر الثاني من عناصر الركن المادي لجريمة التزوير الالكتروني هو :- السند او الوثيقة او المحرر ، حيث لا وجود للتزوير اذا لم ينصب على تغيير الحقيقة في محرر ، ويعرف المحرر بانه " مجموعة من العلامات والرموز التي تعبر اصطلاحا عن مجموعة مترابطة من الافكار والمعاني الصادرة عن شخص او اشخاص معينين "، وهو في جوهره كتابة مركبة من حروف وعلامات تعبر عن معنى او فكرة معينة ، وحسب الاتجاه التشريعي والفقهي الراجح ، يفترض امكان ادراك مادة المحرر بالقراءة البصرية ، وان ينتقل معنى الرموز والعلامات عن طريق المطالعة والنظر ، ومن المسائل الهامة المفترض الاشارة اليها ، والمتصل بموضوع وهدف دراستنا ، ان الفقه متفق على ان فكرة المحرر ، تفترض امكان استشفاف دلالة رموز المحرر بالنظر اليها [78] .

والعنصر الاخر الهام من عناصر المحرر محل التزوير ، اضافة الى اتصاف علاماته ورموزه بثبات نسبي ، هو ان فكرة المحرر ، توجب ان يكشف عن شخصية محرره ، وهذا العنصر مما يتصل بالوظيفة الاجتماعية للمحرر ، والمستقر فقها ان يكون المحرر معبرا عن فكرة بشرية [79].

ولعل العناصر التكوينية لمحل جريمة التزوير التقليدية – المحرر – هي العامل الحاسم في منع انطباق نصوص جريمة التزوير التقلدية على تزوير معطيات الحاسوب (الكمبيوتر) والحاجة الى وضع نصوص خاصة لجريمة التزوير الاكتروني .

وبذلك فلا بد من الاعتراف بان هناك نوعين من المحررات، محررات عادية متعارف عليها عند جمهور الناس، ومحررات ظهرت بظهور ثورة تكنولوجيا الحاسبات وهي ما يطلق عليها بالمحررات الالكترونية، فيراد بالأول هو كل مسطور يحوي علامات او كلمات ينتقل بها الفكر او المعنى من شخص الى اخر بمجرد النظر اليه ويتسم المحرر العادي بثلاث سمات ان يكون متخذاً شكلاً كتابياً طالما هو محرر لابد من ان يكون مكتوباً وبأي لغة تكون محلية او اجنبية ولاعبرة بالمادة التي سطرت عليها الكتابة فقد تكون ورقة او خشب او جلد والقالب المحرر يكون

---

77 اسامة عبدالله قايد ، الحماية الجنائية للمحرارات في جرائم الكمبيوتر ، مرجع سابق ، صفحة 260 .

78 ماجد عمار ، المسؤلية القانونية الناشئة عن التزوير المعلوماتي و وسائل الحماية المتاحه ، دار المهضة العربية ، القاهرة ، 1989، صفحة 199 .

79 نائلة عادل محمد فريد قورة ، جرائم الحاسب الاقتصادية ، دار النهضة العربية ، القاهرة ، 2000 ، صفحة 203 . .

بخط اليد ولكن يمكن ان يكون بالألة الكاتبة او الطابعة كله او بعضه كما يجب ادراك مضمون المحرر بالنظر اليه او لمسه كما ويشترط بأن تكون الكتابة منسوبة لشخص معين معروف او يمكن معرفته كما انه يتسلزم ان يحدث أثر قانوني يتحقق بأستبدال الحقيقة بغيرها بالتحريف او الاصطناع [80] .

اما المحررات الالكترونية فهي سجل أو مستند الكتروني يتم انشاءه او تخزينه او استخراجه او نسخه او ارساله او ابلاغه او أستلامه بوسيلة الكترونية على وسيط ملموس او على أي وسيط اليكتروني اخر ويكون قابلاً للاسترجاع بشكل يمكن فهمه وابراز هذه المحررات الألكترونية الاقراص اللينة والمضغوطة او اية وسائط اليكترونية اخرى [81] .

ونحن بدورنا نرى بان هذا التعريف بين نوعين المحررات العادية و الالكترونية هو خطوة حسنة لتمييز فعل التزوير التقليدي عن فعل التزوير المعلوماتي ، وتكون المدخل للوقوف على العنصر الثالث من عناصر الركن المادي لجريمة التزوير الالكتروني حيث انه يشترط لتحقق ذلك ان يتم تغير الحقيقة في محررات ذات صفة اليكترونية على اعتبار ان التزوير التقليدي يختلف عن التزوير المعلوماتي باعتبار أن الاول جريمة عادية والثاني جريمة الكترونية يشترط لأرتكابها استخدام الحاسب الألي استخدام غير مشروع ، لذلك فأنه يشترط في تغير الحقيقة عند ارتكاب التزوير الالكتروني ان يتم بأستخدام الحاسب الألي لغرض تمييزها عن جريمة التزوير التقليدية ، فالحاسب الالي هو جهاز الكتروني يقوم باداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعة كبيرة تصل الى عشرات الملايين من العمليات الحسابية في الثانية الواحدة، كما بأستطاعته حفظ وتخزين كمية كبيرة من المعلومات والبيانات وأستعمالها وقت الأقتضاء فهذه المميزات هي التي تميز الحاسب الالي عن غيره من الاجهزة الاخرى التي لها القدرة على معالجة البيانات والمعلومات آليا

والكمبيوتر له القدرة والامكانية في ادخال معلومات وبيانات ويتم معالجتها بصورة آلية وهاتين العمليتين يطلق عليهما بالأدخال والمعالجة حيث تعد من ابرز العمليات التي يقوم بها الحاسب الألي ويسهل استخراج نتائج تلك المعلومات واستعادتها وتخزينها لكي يتم الرجوع اليه متى دعت الحاجة مستقبلاً ،ولايستلزم ان يعمل بطريقة معينة على وجه الخصوص ولا يستوجب

80 اسامة عبدالله قايد ، الحماية الجنائية للمحرارات في جرائم الكمبيوتر ، مرجع سابق ، صفحة 266.
81 مدحت رمضان ، الاعتداء على نظم المعلومات ، دار النهضة العربية ، القاهرة ، 2000 ، صفحة 268.

ان يكون مخصص او مصمم لغرض معين وانما يسمى الجهاز حاسب اليكترونيً متى ما قام بوظائفه الثلاث (الادخال، التخزين، المعالجة) للمعلومات والبيانات الواردة في البرامجيات [82].

82 هدى قشقوش ، الائتلاف العمدي لبرامج و بينات معطيات الحاسب الالي ، مرجع سابق ، صفحة 56 .

المطلب الثاني

عناصر الركن المعنوي لجريمة التزوير الالكتروني

الركن المعنوي :- ويتمثل في الإرادة التي يصدر عنها الفعل فهي ارادة آثمة طالما انها أتجهت الى ارتكاب السلوك المجرم وسواء تجسدت في صورة القصد الجنائي في الجرائم العمدية او تجسدت في صورة الخطا في الجرائم غير العمدية [83].

أما الركن المعنوي لجريمة التزوير الالكتروني ، فيتخذ صورة القصد الجنائي . ولا يكفي فيه القصد العام بعنصريه العلم والارادة ، فالقصد العام الذي يقوم على علم المتهم بأركان الجريمة ، واتجاه ارادته الى الفعل المكون لها وتحقيق نتيجته ، تتمثل في تغير الحقيقة في محرر بأحدى الطرق النصوص عليها قانونا ،لا يكفي للقول بتوافر قصد التزوير ، بل تتطلب هذه الجريمة توافر قصد جنائي خاص ، يتمثل بنية استعمال المحرر المزور فيما زور من اجله ، وعلى هذا فان القصد الجنائي في جريمة التزوير التقليدية يعرف على نحو غالب لدى الفقه والقضاء بانه "تعمد تغيير الحقيقة في محرر تغييرا من شانه ان يسبب ضررا وبنية استعمال المحرر فيما غيرت من اجله الحقيقة " [84].

فيجب ان يعلم الجاني انه يغير الحقيقة في محرر باحدى الطرق التي نص عليها القانون واذا كان لايعلم ذلك انتفى القصد الجنائي لدية حتى لو كان جهله راجعا الى اهمالة في التاكد من ذلك،وهذا العلم مفترض فلا يدفع مسئوليته عن ذلك بجهله.كما ينبغي ان يعلم الجاني ان فعلة يسبب ضرارا فعليا او محتملا للغير فاذا انتفى ذلك انتفى القصد ايضاء،ولا يكفي توافر الامرين السابقين بل يلزم بالاضافة الى ذلك ان تتجه نية الجاني الى استعمال المحرر فيما زور من اجله حتى ولو لم يستعمله ولا فائدة من نفي الجاني لهذه التهمة بدفع انه لم يحصل على فائدة من اجراء عمله [85].

والحقيقة ان النص القانوني هو الذي يقرر ما اذا ثمة قصد خاص متطلب لقيام الركن المعنوي وتوافره ام يكتفى بالقصد العام بعنصرية العلم والارادة ، وهذا الامر ينسحب على النص القانوني الخاص بالتزوير الالكتروني كما ينسحب على النص الخاص بالتزوير التقليدي . ومن الامثلة على النص القانوني لجريمة التزوير الالكتروني الذي يتضمن تحديدا للقصد الخاص ، نص

---

83 فوزية عبد الستار ، شرح قانون العقوبات ، مرجع سابق ، صفحة 249 .
84 عمر عيسى الفقمي ، الجرائم المعلوماتية ، بدون دار نشر ، القاهرة ، 2005 ، صفحة 221 .
85 حسام راضي ، حماية المعلومات في ضوء تشريعات التقنية ، دراسة مقارنه ، دار النهضة العربية ، القاهرة ، 2006 .

المادة 12 من قانون مكافحة جرائم تقنية المعلومات العماني رقم 12 لسنة 2011 ، حيث يتضمن النص :- ((يعاقب .... كل من استخدم و سائل تقنية المعلومات فى ارتكاب جريمة تزوير معلوماتى ، وذلك بتغيير الحقيقة فى البيانات أو المعلومات الإلكترونية بالإضافة أو الحذف أو الاستبدال بقصد استعمالها كبيانات أو معلومات إلكترونية صحيحة تكون مقبولة قانونا فى نظام معلوماتى ما)) [86] .

ويتضح من النص المتقدم بأن القصد الجنائي في جريمة التزوير المعلوماتي او الالكتروني يستلزم لتحققه توفر عنصران هما عموماً العلم والارادة ، بعبارة اخرى ان يكون الجاني عالماً بانه يرتكب جرم او سلوك غير مشروع معاقب عليه في التشريعات العقابية ومع ذلك أقدم على ارتكابه، بمعنى يجب ان يكون عالماً بأن ادخال المعلومات والبيانات الى مضمون المحررات او محو تلك المعلومات أو تحويرها أو اتلافها او القيام بأية افعال اخرى من شانها ان تؤدي الى التاثير على المجرى الطبيعي لمعالجة البيانات ولايكفي هذا بل لابد من ان تكون ارادته متوجهة الى احداث النتيجة الجرمية من جراء سلوكه غير المشروع وهي الاضرار بالغير سواء كان اضرار معنوياً ام مادياً ام اجتماعياً ... الخ من الاضرار التي تصيب المصلحة العامة او بمصلحة شخص من الاشخاص [87].

وعليه إذا كان جاهلاً بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق لديه القصد الجرمي وكذلك الحال إذا انتفى علم الجاني بأي ركن من اركان الجريمة فلا يترتب عليه توافر القصد الجنائي لأنه يفترض بالفاعل ان يكون عالماً بكافة اركان جريمته كما قد لا يتحقق القصد الجنائي اذا كان الفعل الذي يقوم به الجاني غير واضح بصورة صريحة كما هو الحال بالنسبة لأنتحال صفة الغير او الاتصاف بصفة غير صحيحة ،ومن ناحية اخرى يستوجب قيام القصد الجنائي في التزوير المعلوماتي ان تكون ارادة الجاني متجهة الى احداث النتيجة الجرمية التي وقعت او اية نتيجة جرمية اخرى وهي الاضرار بالأخرين حتى وان كان هذا الاضرار محتمل الوقوع وعليه فان الركن المعنوي يتحقق في جريمة التزوير المعلوماتي بعلم القائم بفعل التزوير بان الادخال او الاتلاف او المحو أو التحوير للبيانات والبرامجيات المعالجة آلياً يؤدي الى التأثير على المجرى الطبيعي لتلك البيانات او المعلومات وانه قد وقع فعله [88] .

---

86 تركي نعيم شلال ، مرجع سابق ، صفحة 140.
87 تركي نعيم شلال ، مرجع سابق ، صفحة 140.
88 جميل عبد الباقي الصغير ، الحماية الجنائية للمحرارات الالكترونية ، دار النهضة العربية ، القاهرة ، 2003 ، صفحة 189 .

المبحث الثاني

موقف القانون الاردني من جريمة التزوير الالكتروني بوصفها من جرائم انظمة المعلومات

صدر في الاردن مؤخرا قانون جرائم انظمة المعلومات المؤقت رقم 30 لسنة 2010 ، وهو القانون الذي كان منتظرا ان يمثل قانونا شموليا للتصدي لظاهرة الجرائم الالكترونية ومنها التزوير الالكتروني ، لكن وكما سيظهر تاليا ، لم يحقق هذا القانون الغرض المرجو منه ولا الامال التي طال انتظارها منذ ما يزيد على عشر سنوات جرى فيها الاعلان مرارا عن قرب وضع هذا القانون .

وقد سبق اقرار هذا القانون ، سن قانون المعاملات الالكترونية المؤقت رقم 85 لسنة 2001 والذي لا يزال للان مؤقتا ، وهو اول قانون اردني ضمن ما يعرف بتشريعات تكنولوجيا المعلومات - سبقه قانون الاتصالات عام 1995 لكنه لم ينظم القواعد الخاصة بتكنولوجيا المعلومات وجرى لاحقا تعديله وتجري الان اعادة صياغته للتوافق مع متطلبات التطور في حقل تكنولوجيا المعلومات – وقانون المعاملات الالكترونية تضمن ما سمي في ذلك الوقت (النص الاحتياطي) وهو نص المادة 38 منه ، التي جرمت ارتكاب الجرائم التقليدية بوسائل الكترونية ، واعتبر نصا احتياطيا ومؤقتا لحين وضع قانون الجرائم الالكترونية ، ورغم وضع قانون جرائم انظمة المعلومات الا ان هذا النص لم يجر الغاؤه .

وللوقوف على موقف القانون الاردني ومدى كفايته في التصدي لجريمة التزوير الالكتروني ، نتناول تاليا قانون المعاملات الالكترونية (المطلب الاول) ثم نعرض قانون جرائم انظمة المعلومات الاردني من جريمة التزوير الالكتروني (المطلب الثاني)

المطلب الاول

جريمة التزوير الالكتروني في ظل قانون المعاملات الالكترونية

بتاريخ 2001/12/11 سن الاردن قانون المعاملات الالكترونية المؤقت رقم 85 لسنة 2001 ، ليمثل اول قانون اردني ضمن حزمة تشريعات تكنولوجيا المعلومات من جهة ، وثاني قانون عربي في حقل التجارة الالكترونية بعد القانون التونسي ، وقد استند قانون المعاملات الاردني الى الاحكام التي تضمنها القانون النموذجي للتجارة الالكترونية الصادر عن لجنة الامم المتحدة للقانون التجاري الدولي (اليونسترال) ، مضيفا عليه بعض الاحكام فيما يمكن تسميته (الاتمتة المصرفية او التحويلات الالكترونية للاموال) .

وقد نفذ القانون اعتبارا من 2002/4/1 ، حيث اوجبت المادة الاولى منه سريانه بعد ثلاثة اشهر من تاريخ نشره في الجريدة الرسمية (اي من تاريخ 2001/12/31) . وحتى تاريخ اعداد مادة هذا البحث لم يتم وضع الانظمة التنفيذية لهذا القانون علما ان العمل جار لوضع النظام الخاص بانشاء سلطات التوثيق في نطاق خطة عمل وزارة الاتصالات وتكنولوجيا المعلومات لتعديل القانون ووضع انظمته التنفيذية .

وقانون المعاملات الالكترونية شرع لتقرير المساواة بين المعاملات العقدية والتعاملات القانونية التي تتم بوسائل الكترونية وبين تلك التي تتم في البيئة العادية غير الالكترونية ، فساوى بين السجل الالكتروني والعادي ، وبين العقد الالكتروني والعادي ، وبين التوقيع اليدوي والتوقيع الالكتروني ، وبين الرسالة الخطية اليدوية وبين الرسالة الالكترونية ، وهكذا . كما وضع ضوابط واحكام لقانونية ومقبولية وحجية المعاملات الالكترونية والتواقيع الالكترونية .

وبالرغم من ان هذا القانون ليس من القوانين الجزائية ، فقد حرص على النص على عدد من الصور الجرمية والافعال غير المشروعة التي يتصور ارتكابها في بيئة المعاملات الالكترونية ، وهذا امر مفهوم في ظل عدم وجود قانون للجرائم الالكترونية وقت وضع هذا القانون ، فاراد المشرع ان يعزز الثقة بالتعامل الالكتروني ويحمي المتعاملين في نطاقه ، فنص على عدد من الجرائم وقرر لها عقوبات محددة ، وقد وردت هذه النصوص في المواد 35 ولغاية 38 من القانون ، وتتمثل الصور الجرمية محل العقاب بما يلي :-

1- عاقبت المادة 35 كل من يقوم بانشاء او نشر او تقديم شهادة توثيق لغرض احتيالي او لاي غرض غير مشروع بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنتين او بغرامة لا تقل عن (3000) ثلاثة الاف دينار ولا تزيد على (10000) عشرة الاف دينار او بكلتا هاتين العقوبتين . وهذه جريمة تتصل بانشطة التجارة الالكترونية ومحصورة بحالات تقديم شهادة توثيق للتعاملات الالكترونية من جهات لا حق لها في تقديم مثل هذه الشهادة ، ونشير في هذا المقام ان القانون نص على وجوب وضع نظام خاص بسلطات التوثيق لم يتم وضعه للان .

2- عاقبت المادة 36 كل من يقدم الى جهة تمارس اعمال توثيق المستندات معلومات غير صحيحة بقصد اصدار شهادة توثيق او وقف سريانها او الغائها بالحبس مدة لا تقل عن شهر ولا تزيد على ستة اشهر او بغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة الاف دينار او بكلتا هاتين العقوبتين وهذه ايضا صورة جرمية تتصل بالتجارة الالكترونية ومحصورة بخدمات شهادات التوثيق .

3- عاقبت المادة 37 أي جهة تمارس اعمال توثيق المستندات بغرامة لا تقل عن (50000) خمسين الف دينار اذا قامت بتقديم معلومات غير صحيحة في طلب التسجيل او افشت اسرار احد عملائها او خالفت الانظمة والتعليمات التي تصدر استنادا الى هذا القانون. وهذه ايضا صورة جرمية تتصل بالتجارة الالكترونية ومحصورة بخدمات شهادات التوثيق .

4- تمثل المادة 38 ما يعرف بالنص الاحتياطي ، حيث يجري نصها على النحو التالي :-
((يعاقب كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الالكترونية بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة او بغرامة لا تقل عن (3000) ثلاثة الاف دينار ولا تزيد على (10000) عشرة الاف دينار او بكلتا هاتين العقوبتين ، ويعاقب بالعقوبة الاشد اذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون.)) .

وعلى الرغم من ان المواد 35 و 36 و 37 قد تثير بعض التساؤلات كما سنرى ، لكنها لا تمثل تحد بقدر ما تمثله المادة 38 من هذا القانون التي تخلق تساؤلات ذات اتصال بكيفية تطبيق النص في ضوء قواعد قانون العقوبات المستقرة .

فالجريمة الاولى :-

نصت عليها المادة 35 وعالجت جريمة انشاء او نشر او تقديم شهادة توثيق بغرض الاحتيال ،وهذه المادة تجرم السلوك المتمثل [بانشاء او نشر او تقديم شهادة توثيق لغرض احتيالي او لاي غرض غير مشروع] .

وقد تضمن النص من زاوية السلوك ثلاث صور هي :- ، انشاء ، نشر ، تقديم . اما الركن المعنوي ، فان النص صريح في ان يكون قصد الانشاء او النشر او التقديم غرضا احتياليا او أي غرض غير مشروع ، وبالتالي ، فان ارتكاب السلوك لدوافع غير ما ذكره النص ينفي الركن المعنوي للجريمة ، وهو ركن معنوي خاص الى جانب الركن العام بعنصريه العلم والارادة .

الا انه قد اثير بشان هذا النص وهذه الاركان التساؤلات التالية :-

1- ما المقصود بالعمل غير المشروع ؟؟ اهو عمل مجرم وفقا للنظام القانوني الاردني ، ام يكفي ان يقيم العمل مسؤوليات مدنية كما في الفعل الضار الذي الحق ضررا ماديا بآخرين .

2- ما هو معيار التمييز بين التقديم والنشر ؟؟ واذا كانت الشهادة غير حقيقية فان صورتي الانشاء والنشر تتصلان بالشكل الالكتروني في الغالب مع ان النشر قد يتم بواسطة ورقية ، لكن التقديم لا يتصل بهذا الشكل حصرا بل مفهومه المطلق يعني التقديم المادي والالكتروني ، فان كان تقديم مستند ورقي غير حقيقي فيما تضمنه ، افلا نكون امام مصدقة كاذبة مغطاة بموجب التشريع العادي (قانون العقوبات) .

3- وبايجاز ، ما هي اركان هذا الجرم وما هي صور الركن المادي وما الذي يميزها عن بعضها البعض ويميزها عن سلوكيات محل تجريم في نصوص قانون العقوبات .

اما الجريمة الثانية :-

فقد نصت عليها المادة 36 ، وعالجت تقديم معلومات غير صحيحة لاصدار شهادة توثيق ، وعاقبت المادة 36 كل من يقدم الى جهة تمارس اعمال توثيق المستندات معلومات غير صحيحة بقصد اصدار شهادة توثيق او وقف سريانها او الغائها .

ووفقا للنص فان الفرض هنا ان شخصا زود جهة توثيق (رسمية او تجارية) بمعلومات غير صحيحة بغرض التحصل على شهادة توثيق غير صحيحة في مضمونها او بقصد وقف سريان شهادة توثيق صحيحة او الغاء شهادة توثيق صحيحة ، يتمثل الركن المادي :- بتزويد جهة توثيق بمعلومات غير صحيحة ،و يتمثل الركن المعنوي :- قصد خاص (الى جانب القصد العام) وهو الحصول على شهادة توثيق او وقف سريان واحدة او الغاء واحدة .

واهم ما يثار في هذا الصدد ،هو هل وقف سريان الشهادة او الغاؤها يتعلق بشهادة تخص نشاطه هو ام تخص الغير ؟؟ اليس مباحا ان يلغي الشخص شهادة او يوقف سريان شهادة تخصه ؟؟

.

والجريمة الثالثة :-

نصت عليها المادة 37 ، وعالجت قيام جهة التوثيق بتقديم معلومات غير صحيحة في طلب التسجيل او افشاء اسرار العميل او مخالفة الانظمة والتعليمات .

نشير ابتداء ان هذا النص للان معطل بسبب عدم صدور نظام انشاء جهات التوثيق وتبعا لذلك ليس ثمة طلبات تسجيل ولا عملاء لها ولا انظمة او تعليمات حتى تخالف ، ومع ذلك ، فان هذه الجريمة خاصة بجهات التوثيق ، وركنها المادي ان تضمن طلب تسجيلها معلومات غير صحيحة ، او انها خلال ممارستها لعملها تفشي اسرار احد العملاء او تخالف انظمة وتعليمات التوثيق الصادرة بالاستناد للقانون ، ولا يتطلب النص قصدا معنويا خاصا بل تقوم الجريمة بتوفر القصد العام بركنيه العلم والارادة .

وان هذا النص يثير التساؤلات التالية ،هل كل المعلومات المقدمة في طلب التسجيل مناط انطباق لهذا النص ، وهل يشترط فيها ان تحدث ضررا او تجلب نفعا غير مشروع ام لمجرد انها صحيحة (حتى لو كانت بخبرات الشركاء او بعناوينهم) تنشيء الجرم مدار البحث .

كما ان مصطلح افشاء الاسرار يوجب تحديد المعنى المقصود بالسر ، فهل هو السر التجاري المعرف في قانون المنافسة غير المشروعة والاسرار التجارية ؟؟ ام السر مطلقا خاصة ان غالبية الزبائن من الاشخاص الطبيعيين ؟؟ ما هو معيار السر ، وهل البيانات الشخصية (في اطار الحق في الخصوصية) تعد من اسرار العميل ؟؟ ام ان المقصود سلوكيات العميل في البيئة الرقمية وما تعرفه عنه جهة التوثيق بحكم مراقبتها لخطه ومعرفتها بالمواقع التي يتصفحها على الانترنت؟؟ .

واذا ما اعتمد الفقه او القضاء معيارا للسر مناط التجريم بصورة الافشاء الا يتعين ان يكون في اضيق الحدود وبعيدا عن أي قياس لانه محظور في النصوص الجزائية الموضوعية ، وماذا اذا عرفت الانظمة والتعليمات السر ، وغالبا ما سيحصل ذلك ، فهل يعتد بتعريف النظام للسر في وقت ورد نص التجريم بالصورة المطلقة هذه في صلب القانون ؟؟؟

وما يعنينا هنا هو النص التجريمي العام (الجريمة الرابعة) :-

الذي ورد في المادة 38، وهو ارتكاب الجرائم باستخدام الوسائل الالكترونية :- فقد قضت المادة 38 بمعاقبة كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الالكترونية بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة او بالغرامة او كلتا العقوبتين ، وقررت صراحة على انه [[ويعاقب بالعقوبة الاشد اذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون .]]

هذا النص مقرر ايضا بصورة مطابقة تقريبا في التشريعات العربية للتجارة الالكترونية ، خاصة قانوني دبي والبحرين المتاثرين تماما بالقانون الاردني ، وقد اعتبر انه النص الاحتياطي الى حين اعداد قانون جرائم الكمبيوتر او تعديل نصوص العقوبات لتشمل صور جرائم الكمبيوتر .

وفقا لهذا النص ، فان اية جريمة نصت عليها التشريعات النافذة ارتكبت بالطرق الالكترونية تستوجب العقوبة المقررة في النص ، كما انها تستوجب عقوبة اشد ان كان ما يقرره نص التشريعات النافذة للجريمة اشد مما قرره النص ، أي ان من يرتكب اتلافا باستخدام الفايروس يعاقب اما بعقوبة المادة 38 من القانون او بالعقوبة المقررة في النص الخاص باتلاف مال الغير ان كانت اشد .

وان التساؤلات التي تثيرها هذه المادة عديدة ، اهمها :-

1- دخل شخص على نظام كمبيوتر يعود لجهة مصرفية او مالية دون تصريح وتجاوز اجراءات الحماية (كلمة السر وغيرها) ، واحدث بيانا وهميا في النظام بموجبه انشأ لنفسه حسابا بمليون دينار ، ثم قام عبر عمليات تحويل رقمي بنقل مبلغ القيد الى حساباته في بنوك اخرى بصورة حوالات الكترونية وقام بسحب النقود واستولى عليها ؟؟ وفق النص المتقدم ، ما الذي ارتكبه هذا الشخص .

2- **الدخول غير المرخص به للنظام** هل هو معاقب في التشريعات النافذة .

3- اذا اعتبر الدخول من قبيل انتهاك حرمة منزل فهل يجوز اصلا اجراء القياس ، ولو اجزناه جدلا هل هو قياس تتحد فيه العلة .

4- ثم ، انشاء قيد وهمي داخل النظام ، هل سنعتبره مصدقة كاذبة ام تزويرا .

5- نقل القيد الى حسابات عددية ثم سحب المال ، هل هو سرقة .

6- واذا كانت سرقة ، واراد القاضي ان يطبق عقوبة اشد ، باعتبار الجاني ارتكب فعلا خطرا واستولى على مبلغ ضخم (وربما اسرار خطرة) ، فاي صورة من صور السرقة (الجنحية او الجنائية) سيعتمدها ليطبق عقوبتها ، اهي سرقة جنحية ، ام سرقة مشددة ،

واي ظرف تشديد سيعتمد (العنف ، الكسر والخلع ، ام التسور ام غيرها من ظروف التشديد) .

7- هل يمكن القياس في النصوص الجزائية .

8- وما لم تتطابق تماما صورة السلوك العادي المجرم مع السلوك الالكتروني المرتكب هل يمكن تطبيق اية عقوبة اشد مما قرره النص .

وقد اثارت هذه المادة سؤالا قديما خضع لبحث فقهي واسع ، هل يمكن تطبيق النصوص العقابية التقليدية على صور الجرائم الالكترونية المستحدثة ، وحتى نستطيع الاجابة على هذا السؤال لا بد من عرض خلاصة اتجاهات الفقه بهذا الشان ، حتى نتبين ان كان من الممكن فعلا للقاضي الاردني تطبيق نص المادة 38 من قانون المعاملات الالكترونية .

اذا كان الجدل والنقاش اساسه مدى امكان انطباق نصوص القوانين الجنائية التقليدية على الجرائم التي تستهدف الاعتداء على معطيات الحاسوب او المعلومات، فأنه يوجد مواقف فقهية ترفض ذلك و اخرى تؤيده او ترى عدم كفايته من جهة ، وامكان تحققه من نواح اخرى، فان هذا الجدل والذي امتد الى القضاء وحتى جهات التشريع لم يكن بمقدوره اضعاف القناعة السائدة لدى العموم بالحقائق التي افرزتها جرائم انظمة المعلومات بمختلف صورها و اشكالها وان اهم هذه الحقائق من الناحية العملية :- **اولا**، الطبيعة الخاصة لموضوع جرائم الكمبيوتر(المعطيات)، **وثانيا**، الطبيعة المعنوية للمعلومات والمعطيات التي لم تكن فيما سبق محلا للحماية الجنائية او مثارا لتشييد نظريات تتفق وطبيعتها [89].

اما مسألة انطباق نصوص تجريم التزوير في المحررات على تزوير البيانات المخزنة في نظم المعلومات ، او تزوير مخرجات الكمبيوتر رأيين ، احدهما - وهو الرأي الراجح بفعل تبنيه من قطاع واسع من الفقه ، وبفعل تبنيه في التشريعات الجنائية الحديثة في القانون المقارن - يقوم على ان التزوير في المعطيات ، لا يدخل تحت نطاق النصوص التقليدية . اما الرأي الثاني ، فيرى امكان تطبيق النصوص الجنائية المنظمة لجريمة التزوير التقليدية على جرائم تزوير الكمبيوتر [90].

ونتناول بايجاز شديد حجج اصحاب هذين الرأيين ونناقشها فيما يلي :-

---

89 جميل عبد الباقي الصغير ، الحماية الجنائية للمحررات الالكترونية ، دار النهضة العربية ، القاهرة ، 2002، صفحة 188 وما بعدها .

90 يونس عرب ، دليل امن المعلومات و الخصوصية ، جرائم الكمبيوتر و الانترنت ، مرجع سابق ، صفحة 438 .

الاتجاه الاول : عدم امكان تطبيق النصوص الجنائية التقليدية على جريمة التزوير في معطيات الحاسوب .

ابرز متبني هذا الاتجاه الفقيه Ulrich Seiber الذي يرى ان تزوير البيانات المخزنة الكترونيا ، لا ينطوي تحت النصوص التقليدية ، لان نصوص التزوير التقليدية في قوانين اكثر الدول ، كايطاليا والنمسا وسويسرا وفرنسا وبلجيكا ولوكسمبرغ والمانيا (وطبعا قوانين الدول المتأثرة بهذه القوانين كمصر والدول العربية) ، تفترض **امكانية القراءة البصرية** لمحتويات المحرر المدونة فيه ، وهذا غير متحقق بالنسبة لمعطيات الحاسوب المخزنة وعزز رايه هذا من خلال حقيقة ان المستقر في الفقه والقضاء ان الاسطوانه وشريط التسجيل – كما ذكرنا – التي سجلت عليه عبارات ايا كانت اهمتها ، لا تعتبر محررا ، ولا يعد تزويرا تغيير ما سجل عليها[91] .

اما الفقيه jaeger ، فيعزز هذا الرأي لديه ، أن البيانات ، سواء كانت مخزنة في ذاكرة الحاسوب أم منظمة في برامجة او في أشرطة الادخال او الاخراج الممغنطة ، فانها ليست مقروءة بذاتها ، ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق العين البشرية ، اذ أنها تسجل على هيئة جزيئات دقيقة مجهزة ومثبته الكترونيا على دعامة **تتيح للحاسوب** فقط قراءتها ، مما ينفي عنها صفة المحرر . كما ان المعالجة الالكترونية التي يجريها الحاسوب ، وكذلك مخرجاته ، لا تعبر عن فكرة بشرية ، وانما تعبر عن فكرة ميكانيكية للالة [92].

ويؤكد هذا الاتجاه في الفقه الفرنسي ، الفقيه Gassin ، مؤكدا على أن تغيير الحقيقة الذي يقع في الاشرطة الممغنطة ، لا تقوم به جريمة التزوير في المحررات (م 145 فرنسي) لانتفاء الكتابة . ويشاطره الرأي الفقيه Deveze . مع وجوب الاشارة الى أن الفقيه Gassin ، يرى من جانب آخر امكان تطبيق النصوص التقليدية على مخرجات الحاسوب ، لأنها أوراق لها قوة أو قيمة في الاثبات. ويذهب الفقيه الفرنسي Deveze ، عقب اقراره عدم امكان تطبيق النصوص التقليدية لتخلف الكتابة الى أن التغلب على هذه المسألة متاح للقضاء ، اذا غلب روح النصوص على الفاظها وحروفها ، واعتبر ما يظهر على شاشة الحاسوب شكلا مستحدثا للمحرر يمكن أن يقع عليه التزوير [93].

---

91 يونس عرب ، دليل امن المعلومات و الخصوصية ، جرائم الكمبيوتر و الانترنت ، مرجع سابق ، صفحة 438 .
92 يونس عرب ، دليل امن المعلومات و الخصوصية ، جرائم الكمبيوتر و الانترنت ، مرجع سبق ، صفحة 438.
93 يونس عرب ، دليل امن المعلومات و الخصوصية ، جرائم الكمبيوتر و الانترنت ، مرجع سابق ، صفحة 440.

وتعزز هذا الاتجاه الفقهي بتبني القضاء في العديد من الدول ذات الموقف ، وتعزز ايضا باصدار العديد من الدول قوانين خاصة او تعديل قوانينها لتجريم التزوير في معطيات الكمبيوتر ." [94].

الاتجاه الثاني : - امكان تطبيق نصوص التزوير التقليدية على تزوير معطيات الكمبيوتر .

يعتقد بعض الفقه ، ان التغيير الذي يقع على برامج الكمبيوتر او البيانات المخزنة ، يمكن ان تتحقق به في بعض الحالات جريمة التزوير في المحررات ، من هذا الرأي الفقيه البلجيكي Spreutels ويستند لدعم موقفه على ان الفقه الحديث يقبل ذلك بالنسبة للاوراق المقواة المثقبة (من اوائل وسائل ادخال البيانات في الكمبيوترات) ، ويؤيد هذا الرأي في الفقه العربي ، الدكتور عمر الفاروق الحسيني ،ويتبنى رأيه الدكتور جميل عبد الباقي الصغير ، والاستاذ محمد عقاد ، بالاستناد الى ان البرنامج متى دون على اسطوانة او شريط ممغنط يعتبر محررا ، وتغيير الحقيقة فيه يعد بالتالي تزويرا [95].

ويذهب اصحاب الاتجاه الاول الى ان هذا الاتجاه قد جانب الصواب ، فالى جانب الحجج الواردة في موقف الاتجاه الاول ، فثمة خطأ في المساواة بين الاوراق المقواة المثقبة (البطاقات المثقبة) والبرامج ، لان هذه البطاقات يتحقق قراءتها بالعين البشرية وليس باستخدام الكمبيوتر وحده كما هو شأن البرامج التي لا يمكن ادراك محتواها بدون الكمبيوتر ، ثم ان اقرار اصحاب هذا الراي بان المحرر يفترض ان ينتقل معناه الى الشخص المتلقي بالنظر ، وان من عناصره ان يدل بذاته على من ينسب اليه ، تاييد لراي الاتجاه الاول ، لان كلا العنصرين غير متحققين في البرامج والمعطيات. ولعل الراي الذي ذهب اليه الفقه العربي في مطلع التسعينات مرده غياب التدخل التشريعي والسعي الى تطويع النصوص لتوفير الحماية الجنائية ضد مثل هذه الانشطة ، لكن هذا الهدف لا يقبل معه تجاوز مباديء راسخة في القانون الجنائي ، اولها مبدا الشرعية ، وثانيها مبدا حظر القياس في النصوص الجنائية الموضوعية وحظر التوسع فيها ، ولهذا تغير موقف الفقه العربي لدى تدخل المشرع لوضع مثل هذ التشريعات لاحقا [96].

اضافة لما ورد اعلاه من اصحاب الراي الاول ، فاننا نتفق مع الفقه بشان انعدام وجود العناصر الرئيسة لمحل جريمة التزوير التقليدية (المحرر) في معطيات الكمبيوتر وتحديدا عنصر الكتابة المادية ، وعنصر ادراك مضمون المحرر بالنظر ، وعنصر التعبير عن الفكرة البشرية

---

94 يونس عرب ، دليل امن المعلومات و الخصوصية ، جرائم الكمبيوتر و الانترنت ، مرجع سابق ، صفحة 442.

95 يونس عرب ، دليل امن المعلومات و الخصوصية ، جرائم الكمبيوتر و الانترنت ، مرجع سابق ، صفحة 442.

96 يونس عرب ، دليل امن المعلومات و الخصوصية ، جرائم الكمبيوتر و الانترنت ، مرجع سابق ، صفحة 443.

وعلاقة الشخص بالمحرر . كما ان غالبية الفقه القانوني من مختلف النظم ذهب الى عدم انطباق نصوص تجريم التزوير التقليدية على تزوير معطيات الكمبيوتر [97].

وتعزز وتايد هذا الاتجاه مؤلفات الاساتذة التي اشرنا اليها اعلاه . و النص التشريعي من غالبية الدول للنص على هذه الجرائم المستحدثة من جرائم التزوير اما بنصوص خاصة او بتعديل النصوص التقليدية للتزوير، كما هو الشان في الدول العربية التي سنت قوانين في ميدان الجرائم الالكترونية جريا على منهج الدول الغربية والاسيوية وغيرها ، فان نصوص التجريم التقليدية المنظمة لجرائم التزوير ،غير قابلة للانطباق على جرائم تزوير معطيات الكمبيوتر بدلالتها الواسعة[98].

وبالرجوع الى المادة 38 من قانون المعاملات الالكترونية التي تعاقب كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الالكترونية بالحبس ، ووفق غرض النص ، فان جريمة التزوير المنصوص عليها في قانون العقوبات ، اذا ما ارتكبت بوسيلة الكترونية ، فانها تخضع لهذا النص ، واذا كانت نصوص التزوير التقليدي تقيم عقوبات جنحية وجنائية ، فان هذا النص الاحتياطي يقيم عقوبة الحبس حتى سنة ، كما ان التزوير التقليدي وفق النصوص المنظمة له يتوزع الاختصاص بشانه بين محاكم الصلح والبداية بصفتها الجنحية والبداية بصفتها الجنائية ، اما الجرم وفق المادة 38 فانه من اختصاص قاضي الصلح ، اذ لا يملك المدعي العام افتراض ايقاع العقوبة الاشد ليحيلها الى محكمة البداية مثلا .

ثم والاهم من كل ما تقدم ، فان نص المادة 38 سيفتح الباب امام القاضي ليقارب بين الفعل الالكتروني المنظور في الواقعة امامه وبين وسائل التزوير المنصوص عليها في التزوير التقليدي والسابق بيانها ، وهو ما يعني انه سيجتهد في القياس لانه لن يطبق العقوبة الاشد الا بعد ان يتوصل الى ان الفعل يحقق عناصر الجرم المنصوص عليه في قانون العقوبات ، و هذا قياس هو في الاصل محظور على القاضي الجزائي في المواد الموضوعية ، ولهذا لم يطبق هذا النص حتى تاريخه على اي واقعة تتصل بالتزوير الالكتروني .

والقياس الذي سيجريه القاضي ، وهو في الاصل محظور عليه ، لن يقف عند طرق التزوير ، بل سيتعدى ذلك الى اهم عنصر وهو محل الجريمة ، فالتزوير التقليدي كما تقدم اما تزوير (جنائي) في مستندات رسمية ، او تزوير (جنحي بدائي) في اوراق خاصة ، او تزوير

---

97 يونس عرب ، دليل امن المعلومات و الخصوصية ، جرائم الكمبيوتر و الانترنت ، مرجع سابق ، صفحة 444.
98 عبد الفتاح بيومي حجازي ، جرائم الكمبيوتر و الانترنت ، دار الفكر الجامعي ، الاسكندرية ، 2002 ، صفحة 260.

(جنحي صلحي) في مصدقات كاذبة ، في حين محل التزوير الالكتروني ملف او معلومات او بيانات ، فعلى ايها سيقيس القاضي ، وهل يملك مثلا ان يطلب خبرة لبيان طبيعة البيانات او المعطيات الالكترونية وما الذي تمثله ؟؟؟ .

وبالتالي ، ومع ان المادة 38 من قانون المعاملات الالكترونية هدفت الى توفير حماية مؤقتة من الجرائم الالكترونية الى حين سن قانون الجرائم الالكترونية ، فانها في الحقيقة اداة تتناقض مع ضوابط الشرعية الجزائية ومع قاعدة حظر القياس في النصوص الجزائية الموضوعية .

المطلب الثاني

جريمة التزوير الالكتروني في ظل قانون جرائم انظمة المعلومات

صدر في الاردن بتاريخ 2010/8/29 قانون جرائم انظمة المعلومات المؤقت رقم 30 لسنة 2010 بعد اكثر من خمس عشرة سنة انقضت على تقديم العديد من مشاريع القوانين والدراسات التي اعدها خبراء ولجان وجهات متخصصة ساهمت فيها وزارات الداخلية والاتصالات وتكنولوجيا المعلومات واجهزة الامن المختلفة والقضاء وغيرهم ، وقد اصدرت نقابة المحامين مذكرة قانونية حول هذا القانون عقب ورشة عمل متخصصة تناولت احكامه وشارك فيها نخبة من المتخصصين ، وابرز ما خلصت اليه هذه الورشة وتضمنته المذكرة الصادرة عنها ما يلي :-

((وعلى الرغم من الوعي المبكر لاهمية هذا القانون والجهود الخيرة التي تحققت في هذا الاتجاه ، ورغم ان جميع خطط الحكومة منذ عام 2000 والاستراتيجات المتعلقة بتكنولوجيا المعلومات تضمنت **<u>وضع تشريع للجرائم الالكترونية وآخر لحماية الخصوصية</u>** ، الا ان مخرج كل ذلك جاء مخيبا للامال مهدرا لكل هذه الجهود ، اذ جاء قانون جرائم نظمة المعلومات المؤقت رقم 30 لسنة 2010 ابعد ما يكون عن اتجاهات العمل السابقة وبعيدا عن قائمة الحد الادنى من متطلبات مواجهة ظاهرة الجرائم الالكترونية ، قانون هو ادنى مستوى من كل المشاريع المعدة في نطاق اللجان التي عملت على مدى سنوات لوضع اكثر من مشروع واكثر من مسودة ، وهو ادنى مستوى قياسا بسائر القوانين المقارنة المماثلة، ليس فقط قوانين الدول المتقدمة ، بل قوانين دول العالم المصنفة الاقل اقل نموا كالسودان، والاهم انه جاء اقل مستوى من سائر القوانين العربية المماثلة المقرة حتى تاريخ وضعه ، وجاء خارج نطاق معايير الحد الادنى لاتفاقية بودابست (الاوروبية /الدولية) لعام 2001 المتعلقة بالجرائم الالكترونية)) .

ويتكون قانون جرائم انظمة المعلومات من 17 مادة ، المادة 2 وتتعلق بالتعريفات ، والمواد 3- 11 وتتعلق بنصوص التجريم الموضوعية ، والمادة 12 تتعلق بصلاحيات خاصة للضابطة العدلية ، والمادة 13 تتعلق بعقوبة المشترك والمتدخل والمحرض ، اما المادة 14 فتعود مجددا لفكرة النص الاحتياطي (ومشاكله) فتنص على تطبيق العقوبات المقررة في التشريعات النافذة على من يرتكب فعلا باستخدام الشبكة العنكبوتية، واما المادة 15 فتتعلق بالتكرار ، والمادة 16 تتعلق بالادعاء بالحق الشخصي . والمادة 17 تتعلق بنفاذ القانون.

وبالرجوع الى قائمة الجرائم التي عالجتها المواد 3-11 يتبين انها لم تتضمن نصا خاصا بالتزوير الالكتروني ، واكتفى القانون – كمنهج المشرع السعودي مثلا- بتجريم العبث بالبيانات كاثر للدخول غير المصرح به فقط ، هذا العبث الذي قد يتخذ الغاء او تدمير او حذف او تغيير البيانات ، وهو ما نصت عليه المادة 3 من هذا القانون ، وباستثناء هذا النص فان القانون لم يتعرض لتزوير المستندات المعالجة الكترونيا ولا استعمالها ولم يتضمن اي نص يتضمن عناصر جرم التزوير اليت يتعين ان تلحق بسلوك او فعل تغيير الحقيقة ، وهذا واحد من اهم واوضح صور القصور في هذا القانون .

تنص المادة 3 من قانون جرائم انظمة المعلومات على ما يلي :-

((أ-كل من دخل قصداً الموقعٍ الكترونيٍ أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين.

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفتـــه أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين.)))

وبامعان النظر في النص المتقدم ، فانه ابتداء يجرم فعل او سلوك الدخول غير المصرح به الى نظام المعلومات ، وقد عرفت المادة 2 التصريح بانه ((الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو موقع الكتروني أو الشبكة المعلوماتية بقصد الاطلاع أو إلغاء أو حذف أو اضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول اليها أو ايقاف عمل الأجهزة أو تغيير موقع الكتروني أو إلغائه أو تعديل محتوياته)) .

وبالتالي ، فان اي دخول الى نظام المعلومات من الشخص غير الحائز على التصريح بالمعني المقرر في القانون يعد دخولا غير مصرح به ، ويشمل من يملك التصريح ويتجاوز حدود او نطاق الصلاحية التي يتضمنها هذا التصريح .

وينص في الفقرة الثانية من ذات المادة على تشديد العقوبة حين يهدف هذا الدخول غير المصرح به الى واحد من الامور التي ذكرها في النص وهي ((إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفتـــه أو انتحال شخصية مالكه)) .

وبالتالي فان ما تضمنته الفقرة الثانية يعد من قبيل الظرف المشدد ويتعلق بهدف الدخول ونتيجته ، اي يرتبط عضويا بالفعل الجرمي الاساس وهو الدخول غير المصرح به ، وهنا لا بد من ان يثار التساؤل الطبيعي ، ماذا لو كان الدخول مصرحا به ، وبالمعنى المقرر في القانون ، واحدث الشخص تغييرا في الحقيقة في معطيات الكمبيوتر ، فهل يغطي النص هذا الفعل باعتباره تجاوزا لحدود التصريح ام لا يغطيه لاننا امام تغيير للحقيقة بمعنى التزوير في وقت لا ينص القانون على تجريم التزوير ؟؟؟ .

والافعال التي نصت عليها المادة 3 اعلاه – بما فيها من خلل واضح في الصياغة واستخدام المصطلحات كما سنرى – جميعها تستهدف او تقع على :-

1- **البيانات** :- وقد عرفت المادة 2 من القانون **البيانات بانها** " الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليس لها دلالة بذاتها" .

2- **المعلومات** :- وقد عرفت المادة 2 من القانون **المعلومات** بانها " البيانات التي تمت معالجتها وأصبح لها دلالة " .

3- **نظام المعلومات** :- وقد عرفت المادة 2 من القانون **نظام المعلومات بانه** " مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إداراتها " .

4- **موقع الكتروني** :- وقد عرفت المادة 2 من القانون **<u>الموقع الالكتروني</u>** بانه : مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد ."

ومما تقدم ، ظهر لنا اننا امام احد اتجاهين في التزوير الالكتروني ، اما ان يكون محل الجريمة واسعا فيشمل معطيات الكمبيوتر من بيانات ومعلومات (عدا البرامج) او يكون ضيقا فيشمل المستند المعالج الكترونيا فقط . اما افعال العبث بالمعطيات فهي في الحقيقة تشمل كل انواع البيانات والمعلومات وتطبيقاتها المختلفة.

وبالرجوع للنص لا يمكننا ان نضعه في دائرة نصوص التزوير الالكتروني من حيث المحل بل ينطبق عليه التوصيف الخاص بمحل جريمة الدخول غير المصرح به ومحل ظروفها المشددة ، فنص المادة 3 يتحدث عن البيانات والمعلومات والموقع الالكتروني بل يتجاوز ذلك الى النظام نفسه واعمال تعطيله وتدميره .

ايضا النص لا يمكن ان يعد نصا خاصا بالتزوير بالنظر للافعال التي تضمنها، اي الافعال التي تمثل السلوك المكون للركن المادي ، فالافعال التي تضمنها هي ((إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفتـــه أو انتحال شخصية مالكه)) .

وهذه الافعال ليست فقط الافعال التي سبق لنا عرضها كصور للتزوير الالكتروني او باعتبارها العمليات التي تدخل ضمن مفهوم تغيير الحقيقة التي تسهدف المعطيات (بالمعنى الواسع للتزوير الالكتروني) او المستندات المعالجة الكرتونيا (بالمعنى الضيق للتزوير الالكتروني) ، فهذه الافعال تشمل ما يدخل في معنى التزوير والسلوكيات المنتمية اليه وهي :-

1- إلغاء أو حذف أو تدمير او إتلاف أو حجب البيانات والمعلومات .

2- إضافة البيانات والمعلومات .

3- تعديل أو تغيير البيانات والمعلومات .

4- تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته .

لكنها ايضا تشتمل على افعال تقع خارج نطاق التزوير الالكتروني ، وهي :-

1- إفشاء أو نقل أو نسخ بيانات أو معلومات .

2- توقيف أو تعطيل عمل نظام معلومات .

3- إشغال الموقع الالكتروني أو انتحال صفتـــه أو انتحال شخصية مالكه .

ثم ان نص المادة 3 من قانون جرائم انظمة المعلومات انما نص تجريمي للافعال التي تستهدف سرية وسلامة وتوفر المعطيات ، ويوجد مثله في جميع التشريعات المقابلة – مع التنبه للخلل في وصف الافعال وفي الاصطلاحات في النص الاردني ، وكذلك يوجد ما يقابله في اتفاقية بودابست 2001 ، وهذه التشريعات والاتفاقية المذكورة ، والى جانب مثل هذا النص ، تضمنت نصا خاصا بالتزوير الالكتروني خلافا للقانون الاردني .

نخلص مما تقدم ان قانون جرائم انظمة المعلومات الاردني المؤقت رقم 30 لسنة 2010 ، لم ينص على جريمة التزوير الالكتروني ولم ينظمها وانما نظم جريمة العبث بالمعطيات وهي لا تفي بالافعال التي تمثل بحق تزويرا في معطيات انظمة المعلومات وتحتاج عقوبات رادعة .

واجد في هذا المقام الفرصة لابراز اوجه الانتقاد العلمي والموضوعي التي وجهت لقانون جرائم انظمة المعلومات الاردني ، والتي تبنتها ورشة العمل المنعقدة في نقابة المحامين السابق الاشارة اليها ، وانقلها (حرفيا) فيما ياتي :-

((....... نخلص من استعراض النصوص وما يتعين ان تتضمنه القوانين المماثلة الى ان قانون جرائم انظمة المعلومات الاردني المؤقت رقم 30 لسنة 2010 :-

1- لم يتضمن القانون المؤقت نصوص تجريم موضوعية تغطي قائمة الحد الادنى من صور الجرائم الالكترونية المطلوب مواجهتها لخلق لثقة بالبيئة الرقمية ، فلم يجرم :-

- انشطة احتيال الكمبيوتر والاحتيال المالي الالكتروني واكتفى منها بصورة واحدة وهي تلك المتعلقة بالحصول على بيانات البطاقات الائتمانية واستخدامها ، وحتى في سياق البطاقات اغفل صورا جرمية عديدة .

- انشطة التزوير الالكتروني المختلفة ، وهي المنصبة على تعديل ما يعرف بالمستند الالكتروني او اصطناعه وان اشار الى تعديل محتوى الانظمة والشبكات كاثر للدخول غير المصرح به .
- جاء قاصرا في تجريمه لصور الاستيلاء على المعلومات ، فاكتفى بتجريم نسخ البيانات والمعلومات ضمن صورتين ، وبتجريم اطلاع الغير عليها في صورة ثالثة .
- جاء قاصرا بشان جرائم المحتوى الضار ، فلم يجرم سوى بعض صور الجرائم الاباحية وما يعرف بالارهاب الالكتروني او الحض على الارهاب وترويج افكاره وتمويله ، في حين تمتد صور المحتوى الضار الى اكثر بكثير من هاتين الصورتين .
- غابت الصور الجرمية المنضبطة المتعلقة بالسلامة المعلوماتية وعمل المواقع وتعطيلها وانكار الخدمة وسرقة وقت الانظمة واستغلالها غير المشروع وتوزيع الكودات المحمية ووسائل فك التشفير وغيرها .

وهذا النقص لا يمكن تبريره في وقت تمثل جرائم التزوير والاحتيال والاستيلاء على البيانات (بتفرعات انشطتها المختلفة) الصور الرئيسة الثلاث المقررة في جميع القونين المقارنة او تلك المقررة في اتفاقية بودابست لعام 2001 . وفي ذات النطاق غابت العديد من صور التجريم المنضبطة عن الصور لتي نص على تجريمها ، وتفسير هذا القصور انعدام خبرة واضعي مشروع القانون واغفال الجهود السابقة للوزارات والجهات المختصة ، والاعتماد على نقل حرفي لبعض النصوص المقارنة التي ترجع لبدايات ظاهرة الجرائم لالكترونية مع خلل واضح في الترجمة عن النصوص الاصلية التي نقلت .

2- غابت عن قواعد التجريم الموضوعية التي تضمنها القانون **ضوابط الصياغة القانونية الفنية** المفترض توافرها في نصوص التجريم ، فنجد النصوص تستخدم كلمات مترادفة تحمل نفس المعنى في حين يفصلها حرف (او) المشعر باختلافها عن بعضها ، وسبب الخلل انعدام الفهم التقني لصاحب الصياغة، فالافعال التقنية بالنسبة للبيانات والملفات محصورة اما بالانشاء ، او التعديل ، او الالغاء ، او الاستيلاء (ويعالج في نطاقه الاطلاع) ، او الافشاء ، او التحويل والنقل ، او تعطيل الوصول اليه. واية مترادفات لهذه الاصطلاحات يجب الابتعاد عنها او على الاقل اظهار ترادفها بادوات الاضافة المقررة لغة . ولا يقف خلل الصياغة عند هذا الحد بل يمتد لاستخدام مصطلحات تحدث ارباكا دون بيان تعريفها المنضبط مع اننا امام اول قانون للجرائم الالكترونية الذي يحتاج تعريفات لم يتضمنها القانون ، فالمادة 3 مثلا عندما جرمت الاختراق غير المصرح به خلقت فهما خاطئا لدى مستخدمي التقنية وصل حد اعتبار كل دخول

الى موقع الكتروني مخالف للقانون في حين ان التجريم ينصب على انشطة الاختراق لجذر المواقع وللكودات المصدرية بدون اذن وعبر تجاوز اجراءات الامن التقني ، وقد امتد الخلل في الصياغة الى استخدام مفاهيم واصطلاحات مترادفة على انها مختلفة ومغايرة لبعضها البعض ، الى جانب اغفال القانون انه اول تشريع يجرم الافعال الجرمية التقنية وهو ما يستدعي تحديدا دقيق للاصطلاحات الخاصة بعناصر الجريمة ومحلها .

3- القانون ، وفي نطاق قواعد التجريم والعقوبات المقررة لم يراع وجود نصوص تجريم مقررة في قانون الاتصالات (مادة 75 مثلا) وقانون العقوبات وقانون المعاملات الالكترونية المؤقت لعام 2001 (تحديدا المادة 38) لذات الصور او بعضها لتي نص عليها بعقوبات مغايرة ، وهو ما يؤدي الى تناقض التدابير التشريعية في النظام القانوني الواحد . وهذا العيب يظهر اهم خلل في الاداء الحكومي والاداء التشريعي المتعلق بتكنولوجيا لمعلومات ، اذ ليس ثمة رؤيا شمولية وواضحة للقطاع وتدابيره التشريعية وما يحدث في الواقع مجرد حلول جزئية مبتسرة تعكس راي شخوص وليس حكم مؤسسة او موجب نصوص .

4- في شق القواعد الاجرائية جاء القانون خاليا من أهم قواعد التحري والملاحقة وضبط الادلة عبر الشبكات والتعاون الدولي والاقليمي المتعلق بذلك وكذلك قواعد التفتيش وضبط وتحريز الادلة التقنية والاثبات ، وما تضمنه في هذا الشق انحصر في المادة 13 التي منحت جهات الضابطة العدلية صلاحيات (غير منضبطة) لا تراعي معيار التوازن بين فعالية قواعد الملاحقة الاجرائية وبين كفالة وحماية الحريات والحقوق الفردية .

الخاتمة

تناولنا في هذه الرسالة ، وبالقدر الذي يتيحه المقام ، نشأت و تطور التزوير الالكتروني و الاتجاهات التشريعية الدولية والوطنية ، وماهية التزوير الالكتروني (تعريف و محل و صور التزوير الالكتروني ، ثم اركان وعناصر جريمة التزوير الالكتروني و موقف التشريع الاردني من هذه الجريمة في ضوء قانوني المعاملات الالكترونية المؤقت لعام 2001 وقانون جرائم انظمة المعلومات المؤقت لعام 2010 .

ان الاستعراض المتقدم للرسالة يبين لنا الأمور الرئيسة التالية :-

1- التزوير الالكتروني هو جزء من الجرائم الالكترونية ، ويحتاج نصا تشريعا منضبطا يحدد محله ويحدد اركانه وعناصره ضمن تدابير تشريعية تتولى مهمة التصدي لهذه الجرائم .

2- كما أن موضوع التزوير الالكتروني هو موضوع دقيق وشائك ويثير مشكلات جديدة بالنسبة للقانون الجنائي ، مثل مشكلة سريان القانون من حيث المكان ، متمثلة في مدى انطباق القانون الوطني إذا ارتكب في الخارج وإذا تحققت بعض عناصره على اقاليم الدولة وتثور ايضاً مشكلة سريان القانون من حيث الزمان إذا ما ارتكب الجاني الفعل في زمان يصعب تحديده وتحققت نتيجته في وقت اخر قد يصعب تحديده ايضاً، نظراً للتقنية الفنية والبرمجة التي يستخدمها الجاني في ارتكابه، وهنا تثور مشكلة اخرى هي نقطة تحديد بداية السلوك الاجرامي لأحتساب مدة التقادم، و مشكلة مدى انطباق نظام المسؤلية الجنائية بالتعاقب، وايضاً من هم الاشخاص المسؤولين عن هذه الجرائم، ومما تجدر الاشارة اليه ان هذه المشكلات تثار لأن جرائم انظمة المعلومات بصورة عامة وجريمة التزوير الالكتروني بصورة خاصة يصعب السيطرة عليها واكتشافها وتحديد مصدرها او ايقافها بالنظر لسرعة ارتكابها، لذلك كان الزاماً دراسة جوانبها المختلفة وتحليل ايجابياتها ورصد سلبياتها للوقوف على مخاطرها ومعرفة فيما اذا كانت نصوص قانون العقوبات الوطني كافية لمواجهتها ام لا .

3- كما ان جريمة التزوير الالكتروني هي من الجرائم العابرة للحدود وتشكل مجال رحب لمنظمات الجريمة المنظمة ، فهي لم تعد حكر على الافراد المتحمسين لعالم التقنية او

المدركين لأغراءتها ، بل تقع في العديد من الاحيان من قبل الشركات و الموؤسسات اما في ميدان حرب التنافس التجاري او في ميدان نشر الفيروسات في سوق الرمجيات تحت ذريعة حماية المنتج .

4- ان من اهم المسائل التي اثارتها خصوصية هذه الجريمة هو مضمون القواعد الاجرائية التي يجب ان تصبح متلائمة مع طبيعة هذه الجرائم من جهة ، ومن جهة اخرى فأن هذه الجرائم تحتاج لمعرفة متخصصة و تدريب متميز لأعضاء النيابة العامة و الظابطة العدلية و القضاء بكل ما يتعلق بطرق و كيفية استخدام الحواسيب و وسائل التقنية .

5- وبخصوص المعالجة التشريعية الاردنية للتزوير الالكتروني قاصرة وغير فاعلة ولا تتقاطع مع المعايير الدولية واتجاهات التشريعات المقارنة ، فقد غابت تماما عن القانون الاحدث (قانون جرائم انظمة المعلومات الاردني) ، وجاءت غيرذات فعالية في القانون الاسبق (قانون المعاملات الالكترونية) بسبب مخالفة القواعد الثابتة في القانون الجزائي .

6- ان النظام القانوني هو كائن حي يعكس ميول واتجاهات واحتياجات المجتمع ونزعاته للتنظيم ،وذلك لجهة حماية الحقوق الفردية والجماعية عبر قواعد التشريع في فروعه المختلفة ، ومن الطبيعي ان تتاثر علاقاته وقواعد ومرتكزات التشريع فيه بتكنولوجيا المعلومات وما افرزته من آثار اجتماعية واقتصادية وما انتجته او نتج في بيئتها من انماط جديدة للعلاقات القانونية ، ومن الطبيعي ايضا ان تتجه النظم القانونية المختلفة لمعالجة هذه الاثار عبر حركة تشريعية تعكس استجابة التشريع للجديد والمستجد في هذا الحقل ،وبالنتيجة ان تحقيق الحماية القانونية ليس متيسرا دون وجود نظام قانوني فاعل لمواجهة مخاطر الاعتداء على المعلومات ،في ضوء التجدد المستمر لصور واشكال الجريمة المعلوماتية ومنها جريمة التزوير الالكتروني .

التوصيات

في ضوء ما تقدم ، وسندا للدراسات ذات العلاقة ، فان اهم ما نوصي به في هذا الرسالة ما يلي :-

1- وجوب التدخل التشريعي لسن تشريع خاص اكثر تطور لحماية استخدام الكمبيوتر و حماية البينات و البرامج سوا المخزنة او المنقولة عبر شبكات المعلومات ، وان يكون اساس هذا التشريع حماية الحق في المعلومات مع مراعاة التوفيق ما بين موجبات حماية هذا الحق و موجبات تنظيم تداول المعلومات و استخدام التقنية من الكافة بيسر وسهولة ،لذلك ندعو الى الوقوف امام التشريعات القائمة في النظام القانوني واعادة قراءة قدرتها على التواؤم مع متطلبات هذه الاعمال تمهيدا لاصدار حزمة معتبرة ومتكاملة. وان اهم واعظم الحلول فعالية تلك التي تراعي الواقع القائم وتدرك جيدا احتياجاته دون الوقوع في منزلق الحلول والتدابير الجاهزة . وهي حلول وتدابير لن تحقق قدرا من التميز ما لم تكن وليدة انتاج معارفي اصيل لا مجرد مسايرة لمعارف الاخرين .

2- وجوب وضع نصوص تشريعية تجرم الصور الحديثة والمستجدة للتزوير الالكتروني ، والتصدي لصوره التي تحدث اخطارا بالغة تؤثر على الثقة العامة بانظمة المعلومات وشبكات المعلومات وتؤثر سلبا على الاعتماد عليها في وقت اصبحت احد اهم عناصر الانتاج وتقديم الخدمة في القطاعين العام والخاص .

3- لدى النظر في قانون جرائم انظمة المعلومات من قبل السلطة التشريعية بوصفه قانونا مؤقتا ، يتعين على السلطة التشريعية اجراء التعديلات عليه بما يتيح سد اوجه النقص فيه وضبط نصوصه المعيبة واصطلاحاته المستخدمة في غير غرضها ، واذا ما تعذر ذلك فاننا نوصي باعلان بطلان هذا القانون واعادته للحكومة لتقديمه بصورة تتوافق مع احتياجات ومتطلبات الجرائم الالكترونية .

4- تطوير و تحديث قانون اصول المحاكمات الجزائية وذلك بما يكفل مراعاة القواعد الاجرائية المتعلقة بالتحري والأستدلال و التحقيق و جمع الادلة و الظبط والتفتيش التي تتطلبها مثل هذه الجرائم ذات الطبيعة الخاصة والتي تحتاج الى اجراءات خاصة غير متعارف عليها في الجرائم العادية ، حيث لابد من الاعتراف بأن تقنية و تكنولوجيا انظمة المعلومات قد،

اظهرت الحاجة الى الاعتراف بمصالح جديدة ومبتكرة ، واوجبت اعادة تقييم القواعد القانونية والاجرائية في العديد من فروع القانون القائمة لجهة التعامل من انماط السلوك والعلاقات القانونية المستجدة في بيئة تقنية المعلومات .

5- ايجاد الخبرات البشرية المتخصصة بمكافحة جرائم انظمة المعلومات و الاتصالات و الشبكات وجعلها ذراع لين في يد الجهات القائمة على مكافحة هذه الجرائم ، حتى يمكن التصدي لهذه الجرائم عند وقوعها .

6- تشكيل غرف قضائية موكل اليها مهمة النظر بمثل هذه الجرائم و الفصل بها ،مع مراعاة ان يكون السادة القضاة الموكل اليهم مهمة نظر وفصل هذه القضايا ـ مع الاحترام ـ على قدر علي من المعرفة القانونية و التقنية بجرائم انظمة المعلومات بكافة اشكالها و صورها .

7- وجوب الغاء نص المادة 38 من قانون المعاملات لالكترونية لتعارضه مع ضوابط وقواعد التجريم الموضوعي وتحديدا قاعدة الشرعية ومبدا حظر القياس في النصوص الموضوعية ، ولانه كنص احتياطي وفق ما قيل تبريرا له لم يعد كذلك في ضوء وضع قانون خاص بالجرائم الالكترونية .

آمل ان يكون هذا البحث قد اضاء على موضوعه بالقدر الكافي واجاب على مسائل البحث الرئيسة .

والله ولي التوفيق

المراجع

اولاً :- الكتب :-

ابن منظور (ابو الفضل جمال الدين محمد ابن مكرم) ، لسان العرب ، طبعة 1 ، جزء 6 ، منشورات دار صادر ، بيروت ، 1968 .

احمد حسام طه ، الجرائم الناشئة عند استخدام الحاسب الالي (دراسة مقارنه) ، دار النهضة العربية ، القاهرة ، 2000 .

احمد حسام طه تمام ، الحماية الجنائية لتكنولوجيا المعلومات ، دار النهضة العربية ، القاهرة ، 2002 .

اسامة عبدالله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ،(دراسة مقارنه) ، دار النهضة العربية،طبعة 2، القاهرة ،1992

اسامة عبدالله قايد ، الحماية الجنائية للمحرارات في جرائم الكمبيوتر ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، 1996 .

تركي نعيم شلال ، دعاوى التزوير الالكتروني ، دراسة مقارنه ، منشورات الحلبي الحقوقية ، لبنان ، 2000 .

جميل عبد الباقي الصغير، الحماية الجنائية للمحرارات الالكترونية ، دار النهضة العربية، القاهرة، 2002.

حسام راضي ، حماية المعلومات و تشريعات تقنية المعلومات ، (دراسة مقارنه)، دار النهضة العربية ، القاهرة ، 2006.

سعيد عبد اللطيف حسن ، جرائم الكمبيوتر ((جريمة التزوير المعلوماتي)) دراسة مقارنه ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، 1999.

شمس الدين ابراهيم احمد ،وسائل مواجهة الأعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني و المصري، الطبعة الاولى، دار النهضة العربية ، القاهرة ،2005 .

عادل امين ،المؤتمر الثامن للأمم المتحدة لمنع الجريمة ومعاملة السجناء(الواقع والقرارات)،الطبعة الاولى، اتحاد المحامين العرب ، القاهرة، 1991.

عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية، القاهرة 2002 .

عبد الفتاح بيومي حجازي ، جرائم االكمبيوتر و الانترنت ، دار الفكر الجامعي ، الاسكندرية 2002.

عفيفي كامل عفيفي ، جرائم الكمبيوتر ، منشورات الحلبي الحقوقية ، الطبعة الاولى ، بيروت ، 2003 .

عمر عيسى الفقمي ، الجرائم المعلوماتية ، بدون دار نشر ، القاهرة ، 2005 .

فتوح الشاذلي وعفيف كامل عفيف،جرائم الكومبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة والقانون ، (دراسة مقارنة) ، منشورات دار الحلبي الحقوقية ، بيروت، 2003 .

فوزية عبد الستار ، شرح قانون العقوبات – القسم الخاص ، دار النهضة العربية ، الطبعة الثالثة ، القاهرة ، 1990 .

كامل السعيد ، شرح قانون العقوبات الاردني ، الجرائم الواقعة على الاموال ، الطبعة الثانية ، دار الثقافة للنشر و التوزيع ، عمان ، 1991 .

ماجد عمار ، المسؤلية القانونية الناشئة عن التزوير المعلوماتي و وسائل الحماية المتاحه ، دار المهضة العربية ، القاهرة ، 1989.

محمد السعيد رشدى ، الجوانب القانونية لنظم المعلومات ، دار النهضة العربية ، القاهرة ، 2004 .
محمد عبدالله ابو بكر سلامة ، جرائم الكمبيوتر و الانترنت (موسوعة جرائم المعلوماتية) ، دار النهضة العربية ، القاهرة ، 2004 .
محمد علي العريان ، الجرائم المعلوماتية ، دار النهضة العربية ، القاهرة ، 2000 .
محمود نجيب حسني ، شرح قانون لعقوبات – القسم الخاص ، بدون رقم طبعة ، دار النهضة العربية ، القاهرة 1992 .
مدحت رمضان، جرائم الاعتداء على نظم المعلومات، دار النهضة العربية، القاهرة، 2000.
منير محمد الجنبيهى ، جرائم الانترنت و الحاسب الالي و وسائل مكافحتها ، دار الفكر الجامعي ، الاسكندرية ، 2004 .
نائلة عادل محمد فريد قورة ، جرائم الحاسب الاقتصادية ، (دراسة نظرية تاريخية)، دار النهضة العربية ، القاهرة ، 2000 .
نعيم مغبغب ، حماية برامج الكمبيوتر – الاساليب و الثغرات ، دراسة مقارنة ، الطبعة الاولى ، منشورات دار الحلبي ، بيروت ، 2006 .
هدى حامد قاشوش ، الحماية الجنائية لمعطيات الكمبيوتر ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، 2000 .
هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الالات الكاتبة ، اسيوط 1995 .
واثبة داود السعدي ،المعالجة الدولية والوطنية لجرائم الحاسب الالي ، دراسة مقارنة في جرائم تكنولوجيا المعلومات ونظمها المختلفة، ، بدون دار نشر ، بغداد ، 2004 .
يونس عرب ، المدخل الى الجرائم المعلوماتية ، (جرائم الكمبيوتر)، دار النهضة العربية ، القاهرة ، 2009.
يونس عرب ، دليل التعريف في الجرائم الالكترونية ، اتحاد المصارف العرية ، عمان ، 2006 .
يونس عرب ، موسوعة القانون و تقنية المعلومات (1) ، قانون الكمبيوتر ، اتحاد المصارف العربية ، عمان ، 2001 .
يونس عرب ،(دليل امن المعلومات و الخصوصية) ، الجزء الاول ، جرائم الكمبيوتر والانترنت ، اتحاد المصارف العربية ، الطبعة الاولى ، عمان ، 2002.

ثانياً :- الرسائل والبحوث و اوراق العمل :-

سامي الشوا ، الغش المعلوماتي كظاهرة اجرامية مستحدثة ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، 25-28 تشرين الاول ، 1993.

سامي الشوا،جرائم الحاسب الالي والجرائم الاخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال(الانترنت)،ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي،25-28 تشرين الاول 1993 .

عبد الرحيم السلايمة ، التزوير الالكتروني ، بحث مقدم لنقابة المحامبين الاردنيين لغايات استكمال متطلبات التسجيل في سجل المحامين الاساتذة ، عمان ، 2014.

عمر الحسيني ، جرائم الكمبيوتر و الجرائم الاخرى في مجال تكنولوجيا المعلومات ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ، 25-28 تشرين الاول ، 1993 .

كامل السعيد ، جرائم الكمبيوتر و الجرائم الاخرى في مجال التكنولوجيا ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ،25-28 تشرين اول 1993 .

محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي،القاهرة ،25-28 تشرين اول 1993 .

هدى قشقوش ، الاتلاف العمدي لبرامج و بينات الحاسب الالكتروني ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ،25-28 تشرين الثاني1993 .

يونس عرب ، جرائم الحاسوب ، دراسة مقارنة ، رسالة ماجستير مقدمة للجامعة الاردنية ، عمان ، 1994 .

يونس عرب ، الاطار القانوني للارهاب الالكتروني واستخدام الانترنت للاغراض الارهابية ، ورقة عمل مقدمة الى مؤتمر تمويل الارهاب في بيئة الانترنت ، تنظيم جامعة نايف العربية للعلوم الامنية وجامعة القاهرة ، منعقد في جامعة القاهرة ، من 25-27 تشرين اول 2010 .

يونس عرب ، التزوير والاحتيال المالي – الأطر التطبيقية والعلمية و المستجدات الفنية في ظل التطور التكنولوجي ، ورقة عمل مقدمة الى دورة التزوير والاحتيال الالكتروني التي عقدتها مؤسسة الاستشارية لادارة المخاطر و المركز العربي للقانون والتقنية العالية بالتعاون مع شركة كيسنغ الهولندية للنظم المرجعية ، جمعية البنوك في الاردن ، 2004/7/7 .

يونس عرب ، بناء الثقة في البيئة الرقمية في الدول العربية ، دراسة مسحية للتشريعات السيبرانية،منشورات منظمة الاسكوا لدول غرب اسيا ، بيروت ،2010.

يونس عرب ، تطور التشريعات السيبرانية في الدول العربية ، ورقة عمل مقدمة الى ورشة الخبراء الاقليمية حول التشريعات السيبرانية لدى الاسكوا – الامم المتحدة ، 13-14 تشرين ثاني 2013 ، بيروت .

يونس عرب ، قانون انظمة المعلومات الاردني ، ورقة عمل مقدمة ضمن ورشة عمل التشريعات االلكترونية – الاسكوا الامم المتحدة ونقابة المحامين الاردنيين واتحاد المحامين العرب ، عمان ، 8-9 كانون الاول 2013.

يونس عرب ، ورقة عمل ((قانون جرائم انظمة المعلومات) ورشة عمل لمناقشة التشريعات السيبرانية ، نقابة المحامين الاردنيين ، 2010/8/23 .

ثالثأ :- الاتفاقيات و المؤتمرات الدولية :-

1- اتفاقية بودابست الخاصة بالجرائم الالكترونية للعام 2001 .

2- المؤتمر الثامن للأمم المتحدة لمنع الجريمة و معاملة المجرمين ، المنعقد في هافانا – كوبا من تاريخ 27 ايلول – 7 تشرين أول 1990.

رابعاً :- القوانين :-

1- قانون جرائم انظمة المعلومات الاردني المؤقت رقم 30 لسنة 2010 .

2- قانون المعملات الالكترونية المؤقت رقم 85 لسنة 2001 .

3- قانون العقوبات الاردني المؤقت رقم 16 لسنة 1960 .

electronic forgery crime
A comparative analysis study

Done by

Nafel Abed el kareem al Ogla al Faleh.

Supervisor

Dr. Akram Fayez (professor of criminal law.)

The development of information technology applications raging from the invention of the computer and through the PC, not the end of the networks and the internet had the impact in the delevopment of the means to commit crimes ingeneral, including the crime of forgery – mail.

And it is developed in the context of the electronic crimes what is called (Frogery – mail) crime, which relies on the computer as tool to commit and also commited to files and datd stored inside computer systems that is what is cslled mail froud.

In the context of this description the forgery electronic crimes aimed at changing the reality in the files or recoreds or processed documents electronically stored with third parties, or belongs to third parties, or targeting synthesis files that do not exist.The forgery – mail crime is attributed to the range of crimes for which the computer plays the role or a tool that enables and facilities commission of the act, even though the commission of these crimes, begins first by the one of information technology means and applications and went to the address data stored on transmitted via the information system.

And here it is important to stand on the forgery – mail crime ingeneral, its definition, forms, elements, and what falls within its scope, and the relationship between it and between the traditional froud as well as mentioning the most important international and national legislation that governed such a crime.

الملاحق :-

قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010

المادة 1 :

يسمى هذا القانون (قانون جرائم أنظمة المعلومات لسنة 2010)

المادة 2 :

يكون للكلمات والعبارات التالية حيثما وردت في هذا القانون المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك:-

نظام المعلومات: مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إداراتها.

البيانات: الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليس لها دلالة بذاتها.

المعلومات:البيانات التي تمت معالجتها وأصبح لها دلالة.

الشبكة المعلوماتية:ارتباط بين أكثر من نظام معلومات للحصول على البيانات والمعلومات وتبادلها.

الموقع الالكتروني : مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

التصريح :الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو موقع الكتروني أو الشبكة المعلوماتية بقصد الاطلاع أو إلغاء أو حذف أو اضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول اليها أو ايقاف عمل الأجهزة أو تغيير موقع الكتروني أو إلغائه أو تعديل محتوياته.

البرامج:مجموعة من الاوامر والتعليمات الفنية المعدة لانجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات.

المادة 3:

أ-كل من دخل قصداً الموقع الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين.

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفتــه أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين.

المادة 4 :

كل من ادخل أو نشر أو استخدم قصداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الاخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين .

المادة 5 :

كل من قام قصداً بالتقاط أو باعتراض أو بالتنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين.

المادة 6 :

أ- كل من حصل قصدا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الالكترونية يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنتين أو بغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) ألفي دينار أو بكلتا هاتين العقوبتين.

ب-كل من استخدم عن طريق الشبكة المعلوماتية أو أي نظام معلومات قصداً دون سبب مشروع بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الالكترونية للحصول لنفسه أو لغيــره على بيانـات أو معلومات أو أموال أو خدمات تخص الاخرين يعاقب بالحبس مدة لا تقل عن سنـــة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.

المادة 7 :

تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) الى (6) من هذا القانون بحق كل من قام بارتكاب أي منها أثناء تأديته وظيفته أو عمله أو باستغلال أيٍ منهما.

المادة 8 :

أ- كل من أرسل أو نشر عن طريق نظاممعلومات أو الشبكة المعلوماتية قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية يشارك فيها أو تتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة ألاف دينار.

ب-كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية في إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا او عقليا، أو توجيهه أو تحريضه على ارتكاب جريمة، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة الاف دينار.

ج- كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية لغايات استغلال من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا او عقليا، في الدعارة أو الأعمال الإباحية ، يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (5000) خمسة ألاف دينار ولا تزيد على (15000) خمسة عشر ألف دينار.

المادة 9 :

كل من قام قصداً باستخدام الشبكة المعلوماتية أو أي نظام معلومات للترويج للدعارة يعاقب بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة الاف دينار.

المادة 10 :

كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو انشأ موقعاً الكترونياً لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لإتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة.

المادة 11 :

أ-كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع الكتروني أو نظام معلومات باي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني يعاقب بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة ألاف دينار.

ب- إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة ، بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها ، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار

المادة 12 :

أ- مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من الحكمة المختصة، الدخول إلى أي مكان تشير الدلائل الى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص.

ب- مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الاخرين ذوي النية الحسنة، و باستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

ج- للمحكمة المختصة الحكم بمصادرة الأجهزة و الأدوات والوسائل وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة مرتكب الجريمة.

المادة 13 :

يعاقب كل من قام قصداً بالاشتراك أو التدخل أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبيها.

المادة 14 :

كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو أشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع.

المادة 15 :

تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار ايٍ من الجرائم المنصوص عليها فيه.

المادة 16 :

يجوز إقامة دعوى الحق العام والحق الشخصي على المشتكى عليه أمام القضاء الأردني إذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باستخدام أنظمة معلومات داخل المملكة أو الحقت اضراراً بأيٍ من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها ، كليا أو جزئيا ، او ارتكبت من أحد الأشخاص المقيمين فيها.

المادة 17 :

رئيس الوزراء والوزراء مكلفون بتنفيذ أحكام هذا القانون .